ACADEMIA ROMÂNĂ
INSTITUTUL de BIOCHIMIE
Splaiul Independenţei 296, 060031 Bucureşti 17, România Tel: (+40) 21.223.90.69, Fax:(+40)21.223.90.68

MANUALUL POLITICI DE SECURITATEA INFORMATIILOR

COD: PO.IT-02

❒ NECONTROLAT ☑ CONTROLAT ❒ CONFIDENTIAL

1. Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei sau, după caz, a reviziei în cadrul ediţiei procedurii:

Nr. Crt.	Elemente privind responsabilii / operaţiunea	Numele si prenumele	Funcţia	Data	Semnătura
1.1.	Elaborat	Marius Micluta	Responsabil IT	4.12.2017	
1.2.	Verificat	Anca Roseanu	Membru Comisie	11.12.2017	
1.3.	Aprobat	Stefana Petrescu	Director	15.01.2018	

2. Situaţia ediţiilor şi a reviziilor în cadrul ediţiilor procedurii

Nr. Crt.	Ediţia sau, după caz, revizia în cadrul ediţiei	Componentă revizuită	Modalitatea reviziei	Data la care se aplică prevederile sau reviziei ediţiei
2.1.	Ediţia I	Elaborarea ediţiei iniţiale	Conform OSGG 400 / 2015 pentru aprobarea Codului controlului intern/managerial al entităţilor publice	Data aprobării prin decizia Directorului
2.2.				
2.3.				

3. Lista cuprinzând persoanele la care se difuzează ediţia sau, după caz, revizia din cadrul ediţiei procedurii

Nr. crt.	Scopul Difuzării	Exemplar nr.	Compartiment	Funcţia	Nume şi prenume	Data primirii	Semnătura
3.1.	Aplicare	Copie electronică	Consilier Juridic	Consilier Juridic			
3.2.	Informare	Copie elctronică	Comisia monitorizare, coordonare şi îndrumare metodologică a dezvoltării sistemului de control managerial	Presedinte Comisie SCIM	Norica Nichita	15.01 2018	
3.3.	Arhivare	original	Arhivă	Responsabil arhivă	Gabriela Scarneci	15.01. 2018	
3.4.	Aprobare	original		Director executiv	Stefana Petrescu	15.01 2018	

Cuprins

PO.IT-02/01 – Politica de clasificare a informaţiilor

1.1 Politica

Tipuri de informatii in Institutul de Biochimie

1.1.1 **Privat**

Informatii la care au acces numai conducerea Institutului de Biochimie. Este interzisa folosirea sau transmiterea acestor informatii de catre alte persoane care au primit chiar neintentionat acest tip de informatie, pe orice cale. Persoana implicata informeaza imediat proprietarul informatiei.

1.1.2 **Restrictionat**

Informatii la care au acces numai persoane desemnate de catre conducerea Institutului de Biochimie in vederea executarii atributiunilor de serviciu. Informatiile din acesta categorie, au caracter intern si nu pot fi divulgate tertilor decat cu aprobarea scrisa a conducerii Institutului de Biochimie. In caz de scurgere de astfel de informatii se anunta Conducerea institutului.

1.1.3 **Confidential**

Informatie care se incredinteaza numai persoanei care este imputernicita sau autorizata se primesca sau sa o foloseasca.

Toate informatiile legate de relatia Institutului de Biochimie si o persoana angajata cu contract de munca sau contract de prestari servicii sunt confidentiale.

De asemnea sunt cofidentiale toate informatiile transmise si dobandite in comunicarea cu furnizorii, clientii sau tertii. Conditiile de confidentialitate sunt prevazute in contractele Institutului de Biochimie cu aceste parti. De exemplu, in cazul contractului cu un client, informatiile se transmit sau se increditeaza numai persoanelor din organizatia clientului care a fost desemnata de catre conducerea clientului.

Ofertarea prealabila a servicilor se face in baza informatiilor publice. In momentul in care corespondentul este identificat si se detin suficiente informatii despre acesta, cu aprobarea conducerii, se pot transmite informatii suplimentare.

In cazul in care, in procesul de contractare, trebuie divulgate informatii care pot sa afecteze Institutului de Biochimie, cu acordul conducerii se semneaza intre parti Acod de confidentialitate.

Toate documentele Institutului de Biochimie care au inscrise numele celor doua parti au caracter Confidential (de exemplu - factura contract, adrese, informari, notificari etc.)

La transmiterea unei informatii prin email se ataseaza urmatorul text:

"*Acest mesaj si orice fisiere sau documente atasate contin informatii confidentiale, clasificate conform regulilor interne Institutului de Biochimie. Mesajul este destinat doar persoanei sau entitatii adresate si altora autorizati sa-l primeasca. Daca dvs. nu sunteti in aceasta situatie, prin aceasta va informam ca orice dezvaluire, copiere, distribuire sau orice alta actiune bazata pe continutul acestor informatii este strict interzisa si pot fi aplicate sanctiuni, potrivit legii. Daca ati primit acest mesaj din greseala, va rugam sa ne informati imediat si sa stergeti mesajul din sistemul dvs. De asemenea, va rugam sa tineti cont ca transmisia nu poate fi garantata ca fiind sigura sau fara erori. Va multumim!*"

1.1.4 **Informatii cu caracter personal** stabilite de legea datelor cu caracter personal si a procedurii de prelucare a datelor cu caracter personal. Institutului de Biochimie este operator de date cu caracter personal nr …….

1.1.5 **Informatii publice**

Sunt informatii la care poate sa aiba acces oricine:

- publicate pe pagina de web
- oferte nepersonalizate
- materiale publicate in presa
- informatii/ documente aprobate de conducere ca fiind publice

Caracterul *public* al informatiei este stabilit numai si numai de catre conducerea Institutului de Biochimie.

Ca o informatie a Institutului de Biochimie sa devina publica, acesta trebuie sa fi aprobata de catre conducerea Institutului de Biochimie.

Caracterul informatiei poate fi decalarat verbal sau in scris.

Documentele oficiale vor contine categoria informatiei inscrisa pe headerul documentului ca Privat-Restricted-Confidential.

Fiecare angajat trebuie sa aiba semnat un Acord de confidentialitate cu Institutului de Biochimie.

Fiecare colaborator trebuie sa semneze un Acord de confidentialitate cu clauze specifice.

Informaţiile publice sunt cele care au fost declarate ca fiind cunoscute de public de către un angajat autorizat şi care pot să intre în posesia oricui fără a produce pierderi Institutului de Biochimie.

Informaţiile confidenţiale conţin toate celelalte informaţii. Un subset al acestei categorii îl reprezintă informaţiile confidenţiale ale terţilor. Acestea vizează sau aparţin altor organizaţii şi au fost încredinţate Institutului de Biochimie în baza unor clauze contractuale.

Angajaţii Institutului de Biochimie sunt încurajaţi să folosească informaţiile în acord cu clasa din care fac parte. În situaţia în care o informaţie nu este etichetată, angajaţii vor contacta conducerea Institutului de Biochimie.

1.2 Responsabilităţi

Rolurile şi responsabilităţile definite pentru crearea, manipularea şi administrarea informaţiilor stabilesc ierarhia pentru asigurarea conformităţii cu această politică.

1.2.1 Utilizator

Orice persoană care foloseşte informaţiile Institutului de Biochimie ca parte a atribuţiilor de serviciu

Responsabilităţi:

- Respectarea procedurilor de operare stabilite de Director sau custode;
- Prezervarea clasificării informaţiilor în timpul lucrului pentru a se asigura confidenţialitatea, integritatea şi disponibilitatea acestora;
- Folosirea informaţiilor Institutului de Biochimie numai pentru prelucrările autorizate;
- Raportarea activităţilor suspecte sau a încălcării procedurilor şi politicilor de securitate.

1.2.2 Custode

Angajatul care acţionează în numele Institutului de Biochimie

Responsabilităţi:

- Îşi asumă clasificarea informaţiilor;

- Stabileşte controalele necesare pentru asigurarea confidenţialităţii, integrităţii şi disponibilităţii informaţiilor;
- Implementează politicile şi procedurile de securitate;
- Recomandă măsurile corective;
- Identifică şi documentează cerinţele pentru autorizarea accesului la informaţii;
- Comunică cerinţele cu privire la controalele de securitate managerilor şi utilizatorilor;
- Monitorizează conformitatea cu politicile de securitate şi revizuieşte cerinţele cu privire la protecţia informaţiilor;
- Raportează activităţile suspecte sau încălcarea procedurilor şi politicilor de securitate Directorului.

1.2.3 Director/reprezentantul Directorului

Angajatul care creează sau iniţiază crearea sau memorarea informaţiilor (responsabilul procesului)

Responsabilităţi:

- Clasifică informaţiilor conform politicii;
- Realizează inventarul informaţiilor clasificate;
- Se asigură că pentru fiecare nivel de clasificare există măsuri de protecţie;
- Verifică periodic clasificarea informaţiilor.

1.2.4 Responsabilul cu securitatea

Angajatul responsabil cu actualizarea acestei politici şi cu asigurarea infrastructurii necesară sprijinirii custozilor în implementarea şi administrarea controalelor de securitate

1.3 Conformitate

Conducerea Institutului de Biochimie asigură:

- Gestiunea informaţiilor corporatiste, de personal, sau proprietăţile fizice relevante pentru procesele de afaceri, rezervându-şi dreptul de a monitoriza utilizarea tuturor bunurilor Institutului de Biochimie.
- Faptul că toţi angajaţii sunt conştienţi în legătură cu obligaţiile lor de a utiliza informaţiile în acord cu clasificarea lor.

Angajaţii care nu se adaptează la aceste politici vor fi clasificaţi drept persoane care încalcă Regulamentul intern (RI) Institutului de Biochimie şi vor fi supuşi la sancţiuni. Transmiterea şi sau comunicarea de parole persoanelor sau personalului neautorizat este considerată o încălcare a acestor politici.

2 PO.IT-02/02 – Politica pentru comunicaţiile electronice

2.1 Politica

Institutului de Biochimie menţine sistemele electronice de comunicaţii (poştă electronică, poştă vocală, poştă video etc.) pentru a asista procesele de afaceri ale Institutului de Biochimie atât în interiorul cât şi în exteriorul Institutului de Biochimie. Sistemele de comunicaţii luzând echipamentele şi datele stocate sau vehiculate, sunt şi rămân proprietatea Institutului de Biochimie.

- Institutului de Biochimie îşi rezervă dreptul de a primi şi revizui orice mesaj compus, trimis sau primit de oricare dintre angajaţii săi.
- Sistemele de comunicaţii electronice puse la dispoziţie de Institutului de Biochimie pot fi utilizate exclusiv pentru activităţile aprobate de conducerea Institutului de Biochimie.

2.2 Responsabilităţi

- Fiecare angajat trebuie să fie conştient de faptul că în cazul în care un mesaj este eliminat sau şters, este încă posibilă recrearea mesajului în forma sa iniţială; caracterul privat al mesajelor transmise prin sistemul de comunicaţii electronice al Institutului de Biochimie nu este asigurat.
- Chiar dacă accesul în sistemul de comunicaţii electronice se realizează pe baza unui nume de utilizator şi a unei parole secrete, nu se asigură faptul că mesajele tranzacţionate sunt confidenţiale.
- Este strict interzisă crearea sau trimiterea de mesaje prin intermediul sistemului electronic de comunicaţii al Institutului de Biochimie care să aibă un caracter de intimidare, ostil sau care să conţină materiale ofensatoare sau discriminatoare pe bază de: rasă, culoare, origine naţională, crezuri, religie, vârstă, sex, statut familiar, persoane urmărite de lege, dezabilităţi fizice sau mentale, statutul de veteran, orientări sexuale sau altele interzise prin lege (referinţă la RI).

2.3 Conformitate

Conducerea Institutului de Biochimie asigură:

- Gestiunea informaţiilor Institutului de Biochimie, de personal, sau proprietăţile fizice relevante pentru procesele de afaceri, rezervându-şi dreptul de a monitoriza utilizarea tuturor bunurilor Institutului de Biochimie.
- Toţi angajaţii sunt conştienţi în legătură cu obligaţiile lor de a utiliza sistemul electronic de comunicaţii într-o manieră etică şi corespunzătoare.
- Documentarea tuturor variaţiilor cu privire la practicile de securitate stabilite; iniţiază acţiuni corective.

Angajaţii care nu se adaptează la aceste politici vor fi clasificaţi drept persoane care încalcă Regulamentul intern (RI) Institutului de Biochimie şi vor fi supuşi la sancţiuni.

Transmiterea şi sau comunicarea de parole persoanelor sau personalului neautorizat este considerată o încălcare a acestor politici.

3 PO.IT-02/03 – Politica privind accesul la Internet

3.1 Politica

Institutului de Biochimie oferă conexiune la Internet personalului său cu scopul accesării de informaţii, comunicării, primirii şi diseminării de informaţii despre organizaţie sau procesele sale de afaceri. Utilizarea publică a Internetului de angajaţii Institutului de Biochimie este permisă şi încurajată în cazul în care este benefică proceselor de afaceri, într-o manieră consistentă cu Regulamentul intern şi ca o componentă normală de execuţie a responsabilităţilor specifice postului de lucru al angajatului.

3.2 Ghid

1. Utilizarea accesului la Internet oferit de Institutului de Biochimie este permis exclusiv pentru activităţile aprobate de conducerea Institutului de Biochimie.
2. Orice acces la Internet realizat de către angajaţii Institutului de Biochimie trebuie să se desfăşoare conform metodelor oferite de către companie.

3. Responsabilul cu securitatea informaţiilor din cadrul Institutului de Biochimie trebuie să aprobe toate publicaţiile sau conţinutul fişierelor care nu sunt clasificate ca şi informaţii publice în concordanţă cu Politica de Clasificare a Informaţiilor.
4. Regulamentul intern (RI), Conflictul de interese, Protecţia informaţiilor şi a informaţiilor clasificate se aplică de asemenea în utilizarea resurselor Internet oferite de către Institutului de Biochimie
5. Responsabilităţi

Conducerea Institutului de Biochimie asigură:

1. Toţi angajaţii au luat cunoştinţă de existenţa acestei politici.
2. Raportarea tuturor incidentelor de securitate descoperite.
3. Toţi angajaţii au citit şi semnat Declaraţia cu privire la responsabilităţile legate de utilizarea reţelei Internet.

3.3 Conformitate

Angajaţii care nu se adaptează la aceste politici vor fi clasificaţi drept persoane care încalcă ROI Institutului de Biochimie şi vor fi supuşi la sancţiuni.

4 PO.IT-02/04 - Declaraţia cu privire la responsabilităţile legate de utilizarea reţelei Internet

Subsemnatul _____ declar pe propria răspundere că am luat cunoştinţă şi am înţeles că accesul la resursele reţelei Internet, oferit de către Institutului de Biochimie , este destinat exclusiv activităţilor aprobate de conducerea Institutului de Biochimie. Această declaraţie are în vedere şi politicile cu privire la RI şi a Informaţiilor clasificate, fiind interzise printre altele: descărcarea de jocuri, fişiere cu caracter maliţios, materiale inadecvate activităţii specifice postului de lucru, imagini cu caracter obscen sau care nu sunt corespunzătoare activităţii specifice postului de lucru, aplicaţii nelicenţiate.

Sunt conştient şi accept faptul că odată ce am accesat reţeaua Internet, sunt responsabil pentru menţinerea unui standard profesional şi etic ridicat, aşa cum este specificat şi în RI Institutului de Biochimie Am citit şi înţeles politicile menţionate anterior şi accept responsabilităţile mele în protecţia informaţiilor şi reputaţiei Institutului de Biochimie

Data, Numele şi prenumele (în clar),

_____ _____

Semnătura, _____

5 PO.IT-02/05 – Politica privind managementul calculatoarelor şi a reţelei de calculatoare

5.1 Politica

Responsabilităţile cu privire la gestiunea şi operarea tuturor calculatoarelor şi a reţelei Institutului de Biochimie sunt atribuite în maniera următoare:

- În mod clar, fiind documentate toate operaţiunile de operare pentru toate echipamentele pentru a asigura funcţionarea lor corectă şi securizată.

- Procedurile privind responsabilităţile legate de gestiunea incidentelor sunt stabilite pentru a asigura un răspuns rapid, concret şi ordonat, în scopul rezolvării incidentelor de securitate.
- Activităţile de gestiunea şi operarea a resurselor se realizează în conformitate cu regulile de separare a responsabilităţilor cu scopul de a reduce modificările neautorizate sau abuzive asupra sistemului, datelor sau serviciilor.
- Este asigurată segregarea activităţilor de dezvoltare, testare şi utilizare pentru a reduce riscul schimbărilor sau modificărilor accidentale sau neautorizate asupra sistemelor operaţionale sau datelor.
- Riscul, determinat de accesul persoanelor din exteriorul Institutului de Biochimie, care au contracte de gestiune şi întreţinere a anumitor sisteme sau componente de reţea, este identificat şi sunt specificate anumite măsuri de securitate prevăzute în contractele încheiate cu aceştia.

Pregătirea şi planificarea cu scopul prevenirii eventualelor riscuri este organizat pentru a asigura disponibilitatea adecvată a resurselor şi informaţiilor:

- Capacităţile de lucru normale desfăşurării activităţilor de lucru sunt monitorizate şi se asigură o previzionare în timp a necesităţii de prelucrare sau stocare, cu scopul reducerii riscului de supraîncărcare sau suprasolicitare a echipamentelor de procesare sau stocare.
- Sunt stabilite criteriile de acceptanţă şi de testare pentru noile echipamente de calcul sau aplicaţii, înainte de includerea acestora în reţeaua Institutului de Biochimie Sunt implementate măsuri de asigurare a continuităţii afacerii pe o perioadă limitată de timp, pentru fiecare serviciu de reţea, pentru cazurile în care apar anumite disfuncţionalităţi de operare în cadrul sistemului sau acestea sunt determinate de anumite erori fizice apărute la echipamentele de prelucrare.
- Controlul schimbărilor este realizat în aşa fel încât să reflecte în mod clar toate schimbările pentru echipamente, aplicaţii sau proceduri operaţionale.

Procedurile operaţionale obişnuite sunt: crearea copiilor de siguranţă pentru date, jurnale, evenimente şi incidente, monitorizarea echipamentelor şi a mediului de lucru. Pentru îndeplinirea acestora Institutului de Biochimie dispune de:

- Un proces de realizare în mod regulat a copiilor de siguranţă pentru date şi aplicaţii şi asigurarea faptului că aceste date pot fi recuperate cât mai rapid în cazul unor erori fizice sau a mediilor de stocare.
- Un mecanism de jurnalizare a tuturor activităţilor desfăşurate de angajaţi în lucrul la calculator.
- Proceduri de jurnalizare a erorilor raportate de utilizatori cu privire la problemele legate de operarea la calculatoare sau în cadrul sistemelor de comunicaţie, raportare a acestor incidente şi aplicarea măsurilor corective.
- Un proces de monitorizare a mediului de lucru incluzând: temperatura, umiditatea şi calitatea semnalului de energie electrică, pentru a identifica şi elimina eventualele ameninţări adverse care pot afecta lucrul normal la echipamentele de calcul şi pentru aplicarea măsurilor corective.

Securitatea reţelei de calculatoare din cadrul Institutului de Biochimie este organizată şi gestionată cu scopul asigurării protecţiei datelor, informaţiilor şi infrastructurii. Sunt implementate mecanisme de control pentru asigurarea securităţii datelor în timpul transmisiei şi protecţia serviciilor de reţea de accesul neautorizat.

Mediile de stocare a informaţiilor sunt verificate periodic şi protejate pentru a preveni eventuale accidente şi deteriorări care pot conduce la întreruperea proceselor de afaceri. Pentru a asigura acest lucru Institutului de Biochimie dispune de:

- Proceduri de gestionare a mediilor de stocare externă.
- Proceduri pentru manipularea datelor cu caracter confidential în scopul protecţiei acestora de accesul neautorizat, divulgarea sau distrugerea acestora.
- Proceduri de control al accesului neautorizat la documentaţiile sistemului.
- Un proces care asigură stocarea şi depozitarea mediilor de stocare în locaţii sigure şi securizate, atunci când acestea nu sunt utilizate sau când nu mai este nevoie de ele în desfăşurarea normală a proceselor de afaceri.

Schimbul de date, informaţii şi aplicaţii între Institutului de Biochimie şi alte organizaţii este controlat şi monitorizat cu scopul prevenirii pierderilor sau scurgerilor de informaţii, modificarea sau distrugerea acestora. În acest sens Institutului de Biochimie dispune de:

- Convenţii şi contracte formale care includ verificarea aplicaţiilor înainte de acceptarea acestora indiferent de metoda livrării.
- Aplicarea de controale pentru protecţia mediilor de stocare în timpul transportului între diferite locaţii cu scopul minimizării riscului de acces neautorizat, distrugerea sau modificarea datelor.
- Aplicarea, atunci când este cazul, a măsurilor şi controalelor speciale de securitate pentru protecţia schimbului de date între organizaţii, pentru prevenirea interceptărilor sau modificărilor neautorizate.
- Politici şi proceduri clare de control a proceselor de afaceri şi de determinare a riscurilor asociate activităţilor de operare în mediul electronic.

5.2 Responsabilităţi

- Conducerea Institutului de Biochimie are responsabilitatea de a asigura faptul că măsurile aplicate anterior sunt puse în practică, utilizate şi gestionate în mod corespunzător.
- Conducerea Institutului de Biochimie are responsabilitatea de a oferi serviciile necesare responsabilului de proiect pentru punerea în practică a măsurilor specificate anterior.
- Toţi angajaţii care instalează, operează sau întreţin echipamentele de calcul sau de reţea şi aplicaţiile sunt obligaţi să se conformeze acestei politici.

5.3 Scop

Această politică se aplică tuturor serverelor, calculatoarelor, echipamentelor de reţea, aplicaţiilor şi altor dispozitive deţinute şi utilizate de Institutului de Biochimie.

5.4 Conformitate

Conducerea Institutului de Biochimie trebuie să asigure că mecanismele interne de audit există şi monitorizează măsurile dispuse de această politică.

Toti care intră în contact cu serverele, calculatoarele şi reţeaua sunt obligate să respecte prevederile acestei politici.

6 PO.IT-02/06 - Politica cu privire la aplicaţiile de protecţie împotriva software-ului cu caracter maliţios

6.1 Politica

Măsurile de precauţie sunt aplicate pentru a preveni şi detecta încercările de acces în cadrul reţelei Institutului de Biochimie a aplicaţiilor cu caracter maliţios precum şi pentru protecţia integrităţii aplicaţiilor şi datelor. Sistemul de detectare şi măsurile de prevenire a viruşilor precum şi procedurile de informare şi avertizare a utilizatorilor au fost implementate în scopul îndeplinirii prezentei politici.

6.2 Scop

Politica cu privire la aplicaţiile de protecţie împotriva aplicaţiilor cu caracter maliţios se aplică tuturor componentelor IT ale Institutului de Biochimie şi a întregii reţele.

6.3 Responsabilităţi

- Conducerea Institutului de Biochimie are responsabilitatea de a asigura faptul că măsurile enumerate anterior sunt implementate cu eficacitate.
- Responsabilul IT are responsabilitatea de a oferi asistenţă conducerii Institutului de Biochimie în implementarea acestei politici.
- Toţi utilizatorii resurselor IT ale Institutului de Biochimie sunt obligaţi să se conformeze regulilor prezentei politici.

6.4 Conformitate

Conducerea Institutului de Biochimie au obligaţia de a asigura faptul că mecanismele de audit intern existente monitorizează şi măsoară implementarea şi respectarea prezentei politici.

Conducerea Institutului de Biochimie are responsabilitatea de a se conforma acestei politici.

7 PO.IT-02/07 – Politica privind securitatea personalului

7.1 Politica

Securitatea Informaţiei este adresată începând cu stagiului de recrutare, este inclusă în descrierea postului de muncă şi a contractului şi este monitorizată pe toată perioada de angajare în cadrul Institutului de Biochimie Pentru a se asigura respectarea obiectivelor politicii Institutului de Biochimie A asigură faptul că:

- Responsabilităţile de securitate sunt prevăzute în descrierea postului ocupat.
- Aplicaţiile de angajare pentru locurile de muncă ce necesită acces la informaţii importante/sensibile vor fi monitorizate.
- Angajaţii trebuie să semneze un document de confidenţialitate.
- Utilizatorii sunt pregătiţi în procedurile de securitate şi în utilizarea corectă a facilităţilor IT, înainte de a li se da acces la acestea. Totodată ei trebuie informaţi asupra politicilor şi procedurilor de securitate a informaţiilor, a controlului şi a utilizării corecte a facilităţilor IT.
- Incidentele ce afectează securitatea sunt raportate prin diferite canale de comunicaţie către conducerea Institutului de Biochimie cât mai repede posibil. Acest lucru se realizează prin:
  - Raportarea oficială şi aplicarea unui răspuns în caz de incident prin proceduri care identifică acţiunile ce vor fi luate la primirea raportului.
  - Utilizatorii, care sunt conştienţi de faptul că trebuie să noteze şi să raporteze orice activitate suspectă privind o posibilă breşă de securitate sau o ameninţare posibilă asupra sistemului de securitate.

- Utilizatorii, care ştiu cum să noteze şi să raporteze către responsabilul de proiect orice aplicaţie care nu funcţionează corect sau în parametrii normali.

7.2 Scop

Politica privind securitatea personalului se aplica tuturor angajaţilor Institutului de Biochimie, odată cu aprobarea şi implementarea acestei politici.

7.3 Responsabilităţi

- Conducerea Institutului de Biochimie are responsabilitatea de a se asigura că responsabilităţile de securitate sunt prevăzute în fisa postului fiecărui angajat.
- Responsabilul de Resurse Umane are responsabilitatea de a se asigura că celelalte măsuri din această politică sunt îndeplinite cu succes.

7.4 Conformitate

Conducerea Institutului de Biochimie au obligaţia de a asigura faptul că mecanismele de audit intern existente monitorizează şi măsoară implementarea şi respectarea prezentei politici.

Conducerea Institutului de Biochimie are responsabilitatea de a se conforma acestei politici.

Nerespectarea prezentei politicii de securitate sunt referite în politica Disciplina a angajatului Institutului de Biochimie.

8 PO.IT-02/08 - Politica de dezvoltare şi întreţinere a sistemelor

8.1 Politica

Aspectele de securitate sunt incluse pe toată durata de viaţă a unui sistem sau componente a acestuia pornind de la faza de analiză a cerinţelor pentru fiecare proiect de dezvoltare a sistemului. Cerinţele pentru controlul securităţii sunt specificate în declaraţiile cerinţelor de afaceri.

Controalele de securitate sunt proiectate în sistemele de aplicaţii pentru a preveni pierderea, modificarea sau abuzul asupra datelor utilizatorului. Aceste controale sunt:

- Validarea datelor introduse în aplicaţiile de sistem pentru a se asigura corectitudinea informaţiei;
- Incorporarea unor componente de validare în sisteme pentru a detecta o corupere cauzată de erori de procesare sau făcute voit;
- Luarea în calcul a utilizării unei criptări pentru a se asigura confidenţialitatea şi integritatea datelor foarte importante, în timpul transmiterii sau stocării;
- Luarea în calcul a utilizării unui mesaj de autentificare pentru aplicaţiile unde este vitală o protecţie a integrităţii conţinutului.

Pentru a asigura ca proiectele IT şi activităţile de suport sunt realizate printr-o metodă sigură, responsabilitatea pentru accesul la sistemele de fişiere ale aplicaţiei este atribuită utilizatorului care le deţine sau grupului de dezvoltare. Această responsabilitate se concretizează prin:

- Asigurarea unui control strict asupra implementării aplicaţiilor în sisteme;
- Asigurarea protecţiei şi controlului asupra tuturor datelor de test ale aplicaţiilor.

Faza de proiectare şi suport este strict controlată pentru a se menţine securitatea sistemelor de aplicaţii şi a datelor. Acest control ia următoarele forme:

- Control strict asupra schimbărilor de implementare pentru a reduce posibilitatea coruperii sistemelor informaţice;
- Atunci când intervin schimbări asupra sistemului de operare, se cere o revizuire a sistemelor de aplicaţii pentru a se asigura că nu există un impact major de securitate;
- Descurajarea modificării pachetelor de aplicaţii furnizate de producător.

8.2 Responsabilităţi

- Conducerea dezvoltării şi întreţinerii sistemelor Institutului de Biochimie are responsabilitatea de a se asigura că măsurile prevăzute mai sus sunt implementate şi aplicate.
- Responsabilul securităţii informaţiilor are responsabilitatea de a oferi asistenţă Conducerii dezvoltării şi întreţinerii sistemelor în implementarea acestei politici.
- Tuturor angajaţilor implicaţi în dezvoltarea şi întreţinerea sistemelor le este cerută respectarea prezentei politicii.

8.3 Scop

Politica de întreţinere şi dezvoltare a sistemelor se aplică oricărei activităţi ce are legătura cu acest domeniu.

8.4 Conformitate

Conducerea Institutului de Biochimie au obligaţia de a asigura faptul că mecanismele de audit intern existente monitorizează şi măsoară implementarea şi respectarea prezentei politici.

Conducerea Institutului de Biochimie are responsabilitatea de a se conforma acestei politici.

9 PO.IT-02/09 - Politica de control a accesului la aplicaţii

9.1 Politica

Este destinată prevenirii accesului neautorizat la informaţiile din cadrul sistemele informaţice. Utilizatorilor sistemelor de aplicaţii, inclusiv cei care asigură suportul, li se vor da acces la sistemele informatizate şi de aplicaţii, iar acest acces trebuie să corespundă cu cerinţele individuale.

9.2 Ghid

Mijloacele de securitate vor fi utilizate pentru a controla accesul în cadrul sistemelor de aplicaţii. Accesul la aplicaţii şi informaţii va fi permis doar utilizatorilor autorizaţi. Utilizatorilor le va fi acordat doar minimul de acces către informaţii şi aplicaţii, necesar pentru îndeplinirea responsabilităţilor. Sistemele de aplicaţii:

- Vor asigura faptul că au acces la informaţie doar acei utilizatori şi procese cărora li s-a permis acest lucru;
- Vor asigura protecţia împotriva utilizării unor programe ce erijează securitatea sistemului şi aplicaţiilor;
- Vor controla utilizarea altor sisteme cu care informaţiile sunt partajate, schimbate sau eliminate.

9.3 Responsabilităţi

Administratorii şi proprietarii aplicaţiilor trebuie să asigure respectarea acestei politici.

Toţi angajaţii Institutului de Biochimie sau ai oricărei alte organizaţii care are acces la aplicaţii, precum şi deţinătorii informaţiilor şi cei care întreţin şi administrează mijloacele de securitate sunt responsabili în ceea ce priveşte respectarea acestei politicii.

9.4 Scop

Această politică se aplică tuturor angajaţilor: full-time, part-time, cu contract – şi oricăror altor persoane care realizează o colaborare cu Institutului de Biochimie şi au acces la aplicaţii şi informaţii.

9.5 Conformitate

Nerespectarea acestei politici poate determina aplicarea de sancţiuni disciplinare sau desfacerea contractului de muncă.

9.6 Standarde/proceduri suport

Pentru a putea constrânge aplicarea acestei politici Institutului de Biochimie a implementat mai multe standarde/proceduri, printre care:

- Restricţii cu privire la accesul la informaţii;
- Folosirea unor instrumente specifice;
- Controlul accesului la codurile sursă (bibliotecile de resurse);
- Izolarea sistemelor sensibile;
- Clasificarea datelor şi informaţiilor;
- Restricţii de acces la aplicaţii din exterior;
- Existenţa unor cereri de a avea acces pentru utilizatorii externi;
- Suport pentru aplicaţii asigurat de producător;
- Suport pentru aplicaţii şi alte resurse asigurat de terţi pe bază de contracte specifice.

10 PO.IT-02/10 - Politica privind schimbul de date şi aplicaţii

10.1 Politica

Schimbul de informaţii şi aplicaţii între Institutului de Biochimie şi alte organizaţii va fi controlat în concordanţă cu sistemul de clasificare a datelor şi informaţiilor. Acest schimb se va supune reglementărilor şi acordurilor legale şi contractuale. Schimburile vor fi făcute doar în urma unor înţelegeri deja existente. Este necesară aprobarea conducerii şi/sau contractelor legale şi documentat înainte ca schimbul să aibă loc.

10.2 Responsabilităţi

Conducerea Institutului de Biochimie este responsabilă pentru asigurarea respectării acestei politici.

Toţi angajaţii Institutului de Biochimie sau oricărei alte organizaţii – inclusiv cei care deţin informaţiile şi cei care administrează măsurile de securitate – ce au acces la aplicaţiile Institutului de Biochimie sunt de asemenea responsabili pentru respectarea prezentei politicii.

10.3 Scop

Această politică se aplică tuturor angajaţilor: full-time, part-time, cu contract şi oricăror altor persoane care realizează o colaborare cu Institutului de Biochimie şi au acces la aplicaţii şi informaţii.

10.4 Conformitate

Nerespectarea acestei politici poate determina aplicarea de sancţiuni disciplinare sau desfacerea contractului de muncă.

10.5 Standarde suport

Pentru a putea constrânge aplicarea acestei politici Institutului de Biochimie a implementat mai multe standarde şi ghiduri, printre care:

- Securitate pentru e-mail-uri;
- Mesagerie instant;
- Schimb electronic de date (EDI);
- Analiza mesajelor;
- Acorduri de interschimb pentru informaţii şi aplicaţii;
- Securitate pentru mediile de stocare ce se află în tranzit;
- Securitatea sistemelor electronice;
- Sisteme de informaţii publice;
- Alte forme de schimb a datelor.

11 PO.IT-02/11 - Politica privind controlul accesului în reţea

11.1 Politica

Conexiunea la reţeaua Institutului de Biochimie – şi serviciile ce se pot accesa – va fi permisă doar dacă în urma unei comparaţii între nevoile de afaceri ale Institutului de Biochimie şi impactul asupra securităţii reţelei se va decide accesul. Atunci când au loc conexiuni către reţea la date clasificate, sau atunci când utilizatorii ce se conectează sunt într-o zonă cu risc ridicat, este nevoie de aprobarea administratorilor aplicaţiilor respective. Aprobarea pentru conexiunile la reţea şi serviciile acesteia va fi dată astfel încât să îndeplinească un set minim de reguli de acces pentru cerinţele şi specificul aplicaţiei.

11.2 Responsabilităţi

Responsabilul cu protecţia informaţiilor este responsabil pentru respectarea acestei politici.

Toţi angajaţii Institutului de Biochimie sau oricărei alte organizaţii care accesează reţeaua Institutului de Biochimie, precum şi cei care întreţin şi administrează mijloacele de securitate sunt responsabili pentru respectarea acestei politici.

11.3 Scop

Această politică se aplică tuturor angajatilor Institutului de Biochimie, dar şi oricăror alte persoane care întreţin relaţii de afaceri cu Institutului de Biochimie şi au nevoie de acces la reţea pentru derularea proceselor de afaceri.

11.4 Conformitate

Nerespectarea acestei politici poate determina aplicarea de sancţiuni disciplinare sau desfacerea contractului de muncă.

11.5 Standarde suport

Pentru a putea constrânge aplicarea acestei politici Institutului de Biochimie a implementat mai multe standarde şi ghiduri, printre care:

- Acces de la distanţă;
- Acces pentru terţi;
- Autentificarea utilizatorilor;
- Autentificarea la nodurile reţelei;
- Protecţia pe porturi pentru accesul de la distanţă;
- Segmentarea reţelei;
- Control asupra accesului la reţea;
- Control asupra echipamentelor de rutare;
- Securitatea pentru serviciile de reţea;
- Protecţia împotriva aplicaţiilor cu caracter maliţios.

12 PO.IT-02/12 - Politica privind managementul reţelei

12.1 Politica

Standardele, procedurile şi mijloacele de securitate a reţelei vor fi stabilite pentru a proteja reţeaua şi a păstra confidenţialitatea informaţiilor în oricare parte din reţea. Metodele şi procesele de monitorizare a reţelei vor fi realizate pentru a detecta şi reacţiona în cazul unor defecţiuni al reţelei şi în cazul unor încercări de acces neautorizat în reţea. Aprobarea pentru accesul de la distanţă în reţea va fi făcut doar în urma unei evaluări ce va determina că interesele de afaceri şi impactul asupra securităţii reţelei sunt prudente pentru a fi utilizate.

12.2 Responsabilităţi

Administratorul de reţea din fiecare sediu sau filială a Institutului de Biochimie este responsabil pentru aplicarea acestei politici. Acolo unde un sediu nu are un administrator al reţelei, persoana căreia i-a fost dată sarcina de a se ocupa de reţea va avea această responsabilitate.

Toţi angajaţii Institutului de Biochimie sau ai oricărei alte organizaţii care accesează reţeaua Institutului de Biochimie, precum şi cei care întreţin şi administrează mijloacele de securitate sunt responsabili pentru respectarea acestei politici.

12.3 Scop

Aceasta politică se aplică tuturor sediilor şi filialelor Institutului de Biochimie precum şi tuturor celor care întreţin relaţii de afaceri cu aceasta şi au nevoie de acces la reţea.

12.4 Conformitate

Nerespectarea acestei politici poate determina aplicarea de sancţiuni disciplinare sau desfacerea contractului de muncă.

12.5 Standarde suport

Pentru a putea constrânge aplicarea acestei politici Institutului de Biochimie a implementat mai multe standarde şi ghiduri, printre care:

- Routere şi firewall;
- Monitorizare şi Sisteme de Detectare a Intruziunii (IDS);
- Monitorizarea 24⁄7 a tuturor componentelor reţelei;
- Întreţinere de la distanţă pentru componentele cheie ale reţelei.

13 PO.IT-02⁄13 - Politica privind utilizarea şi operare a sistemelor informatice

13.1 Politica

Conducerea Institutului de Biochimie va decide şi documenta, cine are responsabilitatea pentru gestiunea şi operarea tuturor sistemelor informaţice de procesare. Institutului de Biochimie se va documenta asupra procedurilor necesare pentru operarea tuturor sistemelor informaţice de procesare, iar aceste proceduri vor include cerinţe specifice pentru împărţirea şi izolarea sarcinilor de serviciu – nu se va permite ca o singură persoană să controleze mai multe sisteme critice.

13.2 Responsabilităţi

Conducerea Institutului de Biochimie este responsabilă pentru asigurarea respectării acestei politici.

Toţi angajaţii Institutului de Biochimie care utilizează echipamentele computerizate ale Institutului de Biochimie sunt responsabili pentru respectarea prezentei politicii.

13.3 Scop

Această politică se aplică tuturor angajatilor Institutului de Biochimie , dar şi oricăror alte persoane care întreţin relaţii de afaceri cu Institutului de Biochimie şi au nevoie de acces la sistemul de procesare a informaţiilor pentru derularea proceselor de afaceri.

13.4 Conformitate

Nerespectarea acestei politici poate determina aplicarea de sancţiuni disciplinare sau desfacerea contractului de muncă.

13.5 Standarde/proceduri suport

Pentru a putea constrânge aplicarea acestei politici Institutului de Biochimie a implementat mai multe standarde/proceduri, printre care:

- Proceduri operaţionale documentate;
- Controlul schimbării
- Proceduri de gestiune a incidentelor;
- Separarea sarcinilor de serviciu;
- Separarea sistemelor de dezvoltare şi operare.

14 PO.IT-02/14 - Politica cu privire la securitatea fizică

14.1 Politica

Facilităţile de procesare a datelor şi informaţiilor care sunt critice pentru derularea afacerilor Institutului de Biochimie vor fi situate în zone securizate, protejate de un perimetru securizat, cu bariere de securitate şi metode de control a accesului. Aceste metode de control vor fi făcute adecvat astfel încât să restricţioneze accesul la facilităţi doar persoanelor autorizate şi să ofere un control asupra întreruperilor oricăror activităţi ale proceselor de afaceri ale Institutului de Biochimie.

14.2 Responsabilităţi

Conducerea Institutului de Biochimie este responsabilă pentru asigurarea respectării acestei politici.

Toţi angajaţii Institutului de Biochimie care utilizează echipamentele computerizate ale Institutului de Biochimie sunt responsabili pentru respectarea prezentei politicii.

Toţi angajaţii Institutului de Biochimie sau ai oricărei alte organizaţii care accesează reţeaua Institutului de Biochimie , precum şi cei care întreţin şi administrează mijloacele de securitate sunt responsabili pentru respectarea acestei politici.

14.3 Scop

Această politică se aplică tuturor angajatilor Institutului de Biochimie , dar şi oricăror alte persoane care întreţin relaţii de afaceri cu Institutului de Biochimie şi au nevoie de acces la sistemele informatizate pentru derularea proceselor de afaceri.

14.4 Conformitate

Nerespectarea acestei politici poate determina aplicarea de sancţiuni disciplinare sau desfacerea contractului de muncă.

14.5 Standarde/proceduri suport

Pentru a putea constrânge aplicarea acestei politici Institutului de Biochimie a implementat mai multe standarde/proceduri:

- Existenţa unui perimetru fizic de securitate;
- Existenţa unui control fizic al accesului;
- Personal de securitate, camere video, şi alte facilităţi;
- Lucru în zone securizate;
- Locaţii izolate pentru livrare şi încărcare;
- Protejarea echipamentelor;
- Surse de electricitate;
- Cablaje securizate;
- Întreţinerea echipamentelor;
- Securitatea echipamentelor din locaţii externe;
- Eliminarea sau reutilizarea echipamentelor în condiţii de securitate;
- Politica de curăţare a locurilor de muncă şi a monitoarelor.

15 PO.IT-02/15 - Zonarea încăperilor şi spaţiilor de acces

15.1 Politica

Drepturile de acces la informaţii şi servicii se vor baza pe principiul celui mai mic privilegiu care să corespundă nevoilor de derulare a sarcinilor de serviciu. Accesul la informaţii şi date va fi permis doar în concordanţă cu standardele stabilite pentru înscrierea iniţială, întreţinere şi ştergerea dreptului de acces al utilizatorilor.

Posibilitatea trecerii peste oricare din regulile de mai sus se realizează numai în urma unui proces de aprobarea din partea Conducerii Institutului de Biochimie sau a unei persoane împuternicite de şeful de proiect.

15.2 Responsabilităţi

În fiecare sediu al Institutului de Biochimie, persoanele care întreţin resursele de calcul sunt responsabile pentru asigurarea respectării acestei politici.

Toţi angajaţii Institutului de Biochimie sau oricărei alte organizaţii ce accesează reţeaua Institutului de Biochimie , precum şi cei care întreţin şi administrează mijloacele de securitate sunt responsabili pentru respectarea acestei politici.

15.3 Conformitate

Nerespectarea acestei politici poate determina aplicarea de sancţiuni disciplinare sau desfacerea contractului de muncă.

15.4 Standarde suport

Pentru a putea constrânge aplicarea acestei politici Institutului de Biochimie a implementat mai multe standarde şi ghiduri, printre care:

- Detectarea intruziunilor;
- Standarde pentru auditarea drepturilor de acces ale utilizatorilor;
- Gestiunea privilegiilor de acces corelate cu schimbările de la locul de muncă;
- Accesul administratorilor;
- Crearea copiilor de siguranţă şi recuperarea fişierelor ce conţin jurnalul de acces al utilizatorilor;
- Înregistrarea utilizatorilor;
- Sistemul de gestiune al privilegiilor;
- Sistemul de gestiune a parolelor utilizatorilor;
- Revizuirea periodică a drepturilor de acces ale utilizatorilor.

16 PO.IT-02/16 - Conflictul de interese

16.1 Politica

Angajaţilor li se cere să posede standarde înalte de conduită. Pentru a poseda aceste standarde, angajaţii trebuie să aibă un simţ special pentru situaţiile de conflict de interes. Deşi nu sunt întotdeauna cuprinse în lege, aceste situaţii pot dăuna Institutului de Biochimie sau reputaţiei sale.

Un conflict de interese apare atunci când interesele personale ale angajatului intră în conflict cu interesele Institutului de Biochimie. Conflictele de interes pot cuprinde şi relaţiile dintre membrii familiei angajatului şi organizatie. În aceste cazuri de conflict, angajaţi trebuie sa se comporte în bunele interese ale Institutului de Biochimie.

16.2 Standarde

Următoarele standarde pentru un comportament etic au fost stabilite pentru toţi angajaţii ce se află într-o situaţie de conflict de interese:

- Când apare un real sau potenţial conflict de interese, sau când este pe cale să se producă, angajaţii nu trebuie să se implice în acest lucru. Sub nici o formă angajaţii nu trebuie să se implice într-un asemenea mod încât să-i influenţeze în luarea unor decizi ce nu sunt spre bunul interes al Institutului de Biochimie.
- Angajaţii nu vor solicita sau accepta câştiguri personale, privilegii, sau alte beneficii prin implicarea într-un astfel de conflict, din partea Institutului de Biochimie.
- Angajaţii trebuie să îşi concentreze efortul către afacerile Institutului de Biochimie şi vor folosi resursele Institutului de Biochimie doar pentru activităţile aprobate de management. Resursele includ, dar nu numai, echipamente, provizii, informaţii ale Institutului de Biochimie şi timpul pentru care sunt plătiţi să lucreze.

16.3 Responsabilităţi

Angajaţii:

- Oricând se confruntă cu o situaţie de conflict de interese, angajaţii vor cere sfatul superiorilor;
- Atunci când întrebările privind conflictul de interese nu pot fi rezolvate, angajaţii pot cere sfaturi de la Conducerea Institutului de Biochimie;
- Când le este cerut, angajaţii trebuie să dezvăluie actualul sau potenţialul conflict de interese către Institutului de Biochimie.

Conducerea Institutului de Biochimie :

- Managementul de varf va verifica fiecare situaţia şi va sfătui seful de proiect prin acţiunile pe care angajatul va trebui să le facă.

16.4 Situaţii comune de conflict de interese

Situaţiile specifice din aceasta secţiune sunt cele mai întâlnite, în nici un caz ele fiind limitate doar la acestea:

- Cadouri, anumite tipuri de cheltuieli sau alte produse;
- Munca în afara Institutului de Biochimie;
- Interese în alte companii;
- Utilizarea de informaţii confidenţiale;
- Instruirea internă.

17 PS17 - Politica de gestiune a înregistrărilor

17.1 Politica

Aceasta este politica Institutului de Biochimie de a gestiona în mod oportun informaţiile stocate, primite sau create precum şi modul de utilizare şi prelucrare în cadrul diferitelor proiecte desfasurate din companie. Perioada de timp în care înregistrările sunt stocate şi menţinute în companie se bazează pe minimul de timp cerut de reglementările legale în vigoare.

17.2 Responsabilităţi

17.2.1 Centrul de arhivare a înregistrărilor

Rolul centrului de arhivare este de a primi, menţine, distrugere şi întreţinere a înregistrărilor inactive, care nu au termenul de expirare depăşit. Fiecare șef de proiect are responsabilitatea de a stabili propriul calendar de păstrare a înregistrărilor în arhivă în aşa fel încât să se îndeplinească cerinţele minime legale. Procesul de arhivare şi menţinere a datelor se aplică chiar dacă acestea sunt sau nu transferate către centru de arhivare. Copiile calendarului de păstrare şi transfer a înregistrărilor trebuie menţinute în fiecare proiect în scopul inspecţiilor periodice.

17.2.2 Gestionarul înregistrărilor

Gestionarul înregistrărilor are rolul de a administra sistemul de gestiune a înregistrărilor. El trebuie să fie familiarizat cu toate tipurile de înregistrări şi/sau grupuri de înregistrări din cadrul Institutului de Biochimie şi are cunoştinţe ridicate cu privire la toate aspectele activităţii de gestiune a înregistrărilor. Responsabilităţile gestionarului înregistrărilor includ planificarea, dezvoltarea şi administrarea politicilor de gestiune a înregistrărilor. De asemenea, anual, trebuie să organizeze un inventar al tuturor înregistrărilor din cadrul Institutului de Biochimie care trebuie efectuat împreună cu responsabilul de proiect.

17.2.3 Managerul de personal

Managerul de personal este responsabil de toate înregistrările care se află sub controlul său.

17.2.4 Coordonatorul de înregistrări

Coordonatorul înregistrărilor asigură legătura dintre responsabilul de proces/proiect şi centrul de arhivare a înregistrărilor. Este recomandat ca pentru fiecare proiect să se numească un coordonator al înregistrărilor. Documentul de numire al coordonatorului înregistrărilor trebuie să conţină: Numele şi prenumele complet, numărul de telefon. Documentul de numire a coordonatorului este trimis şi păstrat la centrul de arhivare a înregistrărilor. O copie a documentului este înmânată responsabilului şi una şefului de proiect.

17.3 Conformitate

Conducerea Institutului de Biochimie asigură:

- Gestiunea informaţiilor corporatiste, de personal, sau proprietăţile fizice relevante pentru procesele de afaceri, rezervându-şi dreptul de a monitoriza utilizarea tuturor bunurilor Institutului de Biochimie.
- Faptul că toţi angajaţii sunt conştienţi în legătură cu obligaţiile lor de a utiliza informaţiile în acord cu clasificarea lor.

Angajaţii care nu se adaptează la aceste politici vor fi clasificaţi drept persoane care încalcă Regulamentul intern Institutului de Biochimie şi vor fi supuşi la sancţiuni. Transmiterea şi sau comunicarea de parole persoanelor sau personalului neautorizat este considerată o încălcare a acestor politici.

18 PO.IT-02/18 – Regulile şi conduita IT în cadrul Institutului de Biochimie

18.1 Politica

Se presupune că angajaţii Institutului de Biochimie se poartă într-un mod profesional mereu, când sunt în cadrul Institutului de Biochimie sau când reprezintă Institutului de Biochimie

In cadrul acestui document vor fi listate regulile de baza care trebuie respectate în cadrul Institutului de Biochimie precum şi îndrumări privind conduita angajatului Institutului de Biochimie. Aceste reguli sunt grupate în seturi de reguli ce formează o anumită politică. în principal sunt patru politici de baza şi anume:

1. E-mail Security Policy
2. Protecţia Informaţiilor
3. Instalarea şi întreţinerea programelor Antivirus
4. Politica de Internet.

18.2 E-Mail Security Policy

Sistemul electronic de email este destinat să furnizeze comunicaţii eficiente între toţi angajaţii Institutului de Biochimie precum şi între aceştia şi partenerii de afaceri ai Institutului de Biochimie . Acest sistem este un instrument de mare productivitate dar care şi expune Institutului de Biochimie la riscuri privind transmiterea de mesaje peste reţele publice şi locale. Obiectivul acestei politici este să asigure înţelegerea acestor riscuri precum şi a modalităţilor de folosire şi protecţie a sistemului şi a informaţiilor.

18.2.1 Politica de e-mail agreata şi acceptata

a) Sistemul de e-mail este proprietatea Institutului de Biochimie . Sistemul include softul de email, server hardware, reţele, căsuţele poştale, adresele, user IDs şi parole. Toate mesajele sunt înregistrări ale Institutului de Biochimie.

b) Sistemul de email va fi utilizat pentru nevoile de afaceri ale Institutului de Biochimie şi ca o sursă de informaţii şi comunicare eficientă de către angajaţi şi conducere. Utilizarea în scop personal este admisă numai ocazional.

c) Utilizatorii sistemului de e-mail îşi vor proteja conturile cu o parola ce îndeplineşte standardele definite în politica de securitate a Institutului de Biochimie.

d) Angajatii pot revizui comunicaţiile celor ce folosesc sistemul de email pentru a se asigura că politica de securitate stabilită este respectată, şi/sau pentru a stabili eventualele acţiuni neautorizate în sistemul de comunicaţii.

e) Institutului de Biochimie îşi rezervă dreptul de a monitoriza mesajele de email şi de a face cunoscut conţinutul acestora către autorităţile legale fără a notifica în prealabil utilizatorul, dacă situaţia necesită acest lucru.

f) Urmatoarele sunt situatii de folosire neadecvata a sistemului:

- incercari neautorizate de access la conturile altor utilizatori
- trimiterea de mesaje din contul altui utilizator fara a avea permisiunile necesare de a face acest lucru
- transmiterea de informaţii confidentiale Institutului de Biochimie către persoane neautorizate sau alte organizatii.

- Transmiterea în mesaje (altele decat în scopuri de cercetare supravegheata şi legala) a imaginilor sau datelor ofensatoare, obscene sau indecente.
- crearea sau transmiterea de materiale care sunt create pentru a cauza neplaceri, inconveniente sau anxietate nejustificata
- crearea sau transmiterea de materiale abusive sau care reprezinta o ameninţare, hartuiesc sau intimideaza pe altii.
- crearea sau transmiterea de materiale care discrimineaza sau incurajeaza discriminarea rasiala sau etnica, pe principii de sex, orientare sexuala, statut civil, dizabilitati, orientari politice sau religoase.
- crearea sau transmiterea de materiale calomnioase
- crearea sau transmiterea de materiale care includ plangeri false sau de natura deluzorie
- utilizarea de termeni sau limbaj nepoliticos, care include termeni ofensivi sau condescendenti
- activităţi care violeaza intimitatea altor utilizatori
- crearea sau transmiterea de mesaje anonime, fara identificarea clara a transmitatorului
- Transmiterea de mesaje tip junk-email, chain-letter sau de mesaje de business în scop personal
- Folosirea e-mailului în scopuri ilegale.

18.2.2 Reguli şi îndrumări de utilizare

a) confidentialitatea mesajelor dvs nu poate fi garantata! Mesajele dvs pot fi forwardate de către destinatar către alte terte persoane. De aceea adoptati în mesajele dvs o atitudine conforma cu cea a unui “public meeting”.

b) Mesajele de email creaza o inregistrare. Deoarece se fac copii de backup de către administratori, mesajele sunt pastrate ca inregistrari chiar dacă dvs le-ati sters din casuta dvs. De aceea tratati mesajele de e-mail ca şi cum ar fi inregistrari permanente.

c) Fiti constienti de faptul ca mesajele odata trimise nu mai pot fi retrase. De aceea evitati mesajele emotionale care pot fi percepute în mod negativ de către destinatar.

18.2.3 Violarea politicii de e-mail

Institutului de Biochimie va revizui cazurile de violare a politicii de e-mail şi va actiona în functie de cazul respectiv, actiunile Institutului de Biochimie putand merge de la notificarile în scris către userul respectiv pana la pierderea drepturilor de a folosi emailul si/sau computerele Institutului de Biochimie, sau chiar pana la actiuni disciplinare de tip suspendare sau terminare a contractului de munca cu posibila atentionare a autoritatilor legale.

18.3 Protecţia informaţiilor

Protectia informaţiilor se refera la protectia datelor Institutului de Biochimie, a aplicatiilor sistemelor şi resurselor de reţea contra eventualelor alterari, distrugeri sau scurgerilor deliberate de informaţii.

Se considera resurse de informaţii urmatoarele:

1. Documentatii sau comunicari printate sau scrise cum ar fi rapoarte, scrisori sau memorii.
2. Tranzactiile online (Online screen transactions)
3. Aplicatiile Software
4. Fişiere de tip “seturi de date” sau baze de date care pot fi pe orice media.
5. Sistemele de procesare ce include serverele, CP-urile, workstation-urile şi imprimantele
6. Resursele de reţea

Important: Este responsabilitatea fiecăruia de a preveni folosirea neautorizată a informaţiilor, distrugerea sau scurgerea de informaţii. Fiecare utilizator este obligat să protejeze informaţiile şi resursele de informaţii ale Institutului de Biochimie.

18.3.1 Responsabilităţile utilizatorului:

Orice utilizator al computerelor/ sistemelor Institutului de Biochimie este responsabil în ceea ce priveste pastrarea confidentialitatii şi integritatii datelor de companie la care el/ea are access.

Avand un user ID sunteti responsabil(a) pentru pastrarea confidentialtatii parolei de access şi de asemeni pentru orice actiune care a avut loc din partea ID-ului ce il detineti.

Urmatoarele reguli de conduita sunt obligatorii:

1. Utilizatorii au obligaţia de a citi şi a cunoaşte prevederile acestui regulament. Neştiinţa şi ignoranţa nu pot fi folosite drept scuză pentru cauzarea de disfuncţionalităţi ale reţelei sau încălcări ale regulamentului sau a legislaţiei în vigoare.
2. User ID şi parola sunt personale, nu se imprumuta şi nu se comunica altora. Personalul este responsabil pentru orice actiune intreprinsa de ID-ul lui.
3. Nu vor face publice informaţii legate de structura şi organizarea retelei Institutului de Biochimie.
4. Setarea unei parole compusa atat din litere dar şi cifre pentru a fi mai greu de ghicit. Lungimea parolei trebuie sa aiba minim 8 caractere şi va trebui schimbata la cel puţin 60 zile. Nu se pun în parole nume obişnuite sau date de nastere ce pot fi ghicite usor.
5. Se memoreaza parola şi se evita scrierea.
6. Cand se parasese statia pe care se lucreaza, chiar şi pentru scurt timp, se efectueaza Lock (blocarea statiei ALT+CTRL+DEL urmat de tasta K) sau chiar LOGOUT.
7. Se pastreaza toate documentele continand date confidentiale în locuri special destinate cum ar fi cabinete şi birouri incuiate sau camere speciale.
8. Dacă se banuieste ca parola a fost compromisa, se schimba imediat şi se anunta seful direct şi administratorul de reţea. Dacă nu se poate schimba parola, se anunta pe administratorul de reţea pentru resetare.
9. Se raporteaza orice activitate neobişnuita, brese în securitate sau practici care nu asigura securitatea datelor Institutului de Biochimie superiorului ierarhic.
10. Datele Institutului de Biochimie sunt numai pentru utilizarea lor în cadrul afacerilor Institutului de Biochimie. Utilizarea lor în alte scopuri decat acelea pentru sunt emise autorizatii este interpretat ca o utilizare gresita.

11. Utilizatorii trebuie sa previna introducerea de viruşi pe statiile lor de lucru. Jocurile, fişierele aduse de pe internet de tip games, soft-uri aduse de acasa sunt interzise deoarece creste riscul introducerii de viruşi în reţea.
12. Nu se instaleaza pe statiile de lucru decat programele stabilite de către management pentru buna desfasurare a activităţii. Orice alt program sau utilitar aditional se va instala numai cu acordul superiorului. Angajatii Institutului de Biochimie vor utiliza în reţea date şi software numai în conditiile respectarii regulilor de copyright şi licentiere al posesorilor acestora.
13. Utilizatorii vor respecta regulile stabilite de administratorii altor retele externe atunci cand acceseaza resursele acestora, precum şi regulile stabilite prin prezentul regulament şi de legislatia în vigoare.
14. Utilizatorii vor respecta caracterul personal al datelor şi calculatoarelor aparţinând celorlalţi utilizatori.
15. Utilizatorii reţelei Institutului de Biochimie au dreptul la confidenţialitate asupra corespondenţei şi datelor pe care le deţin în Institutului de Biochimie. Totuşi, ei trebuie să accepte un grad rezonabil de asigurare a acestui drept. În plus, utilizatorii trebuie să accepte dreptul conducerii Institutului de Biochimie de a accesa informaţiile personale, atât pentru administrarea reţelei, cât şi în scopul verificării respectării regulilor stabilite prin acest regulament precum şi a legislaţiei în vigoare.
16. Regulile de conduită stabilite de prezentul regulament sunt acceptate liber, prin consimţământ scris, de către fiecare utilizator în parte, în momentul dobândirii calităţii de utilizator. Nerespectarea lor ulterioară atrage după sine pierderea fără o notificare prealabilă a calităţii de utilizator şi răspunderile civile şi penale corespunzătoare regulamentului de funcţionare Institutului de Biochimie şi legislaţiei în vigoare.

Sunt interzise urmatoarele activităţi în cadrul Institutului de Biochimie:

1. promovarea de activităţi comerciale neautorizate
2. generarea de trafic excesiv care împiedică funcţionarea reţelei în condiţii normale
3. transferuri de materiale pornografice
4. transferuri de materiale care contravin legilor drepturilor de autor (software piratat, filme, muzică etc.)
5. tentative de exploatare a problemelor de securitate care pot apărea (accesul, alterarea sau ştergerea neautorizată a datelor sau software-ului, răspândirea de aplicaţii informaţice din categoria software-ului maliţios: viruşi, troieni, viermi, spyware etc.)
6. distrugerea sau încercarea de a distruge securitatea sistemelor de calcul
7. compromiterea sau tentativa de compromitere a integrităţii sistemelor de calcul
8. hărţuirea altor utilizatori
9. utilizarea resurselor, în particular poşta electronică, servere de web şi buletine pentru a transmite mesaje obscene, repetate, frauduloase sau nesolicitate, cu caracter comercial (de exemplu spam).
10. utilizarea de software necunoscându-se efectele pe care le produce

Exemple de activităţi interzise se gasesc în Anexa 1 de la sfarsitul acestui document.

18.4 Instalarea şi întreţinerea programelor Anti-Virus

Institutului de Biochimie este protejata contra viruşilor prin sistemul de firewall al Institutului de Biochimie precum şi de firewall-urile locale ale sistemelor de operare de pe pc-uri. Protectia online şi scanarea anti-virus este realizata de sistemul corporate Symantec atat ca server/client pentru pc-urile din cadrul Institutului de Biochimie cat şi pentru serverul de email (scanarea fluxurilor smtp intrare-iesire).

Reguli de conduita şi obligatiile utilizatorilor:

1. In caz ca utilizatorul nu se descurca cu instalarea clientului de antivirus pe care Institutului de Biochimie il pune la dispozitie, este obligat sa ceara Asistenţă din partea administratorilor de reţea.
2. Dupa instalare utilizatorul este obligat sa verifice ca antivirusul este updatat la zi (in mod automat) şi dacă acest lucru nu se intampla în timp rezonabil (max 30 min) atunci va trebui sa anunte un administrator de reţea.
3. In sarcina utilizatorului intra obligatia verificarii periodice a calculatorului (scanare) precum şi a verificarii updatarii semnaturilor. în cazul aparitiei de probleme, utilizatorul trebuie sa contacteze un administrator de sistem al Institutului de Biochimie.
4. Firewall-ul local al sistemului de operare trebuie mentinut intotdeauna activat, exceptiile sunt permise doar în reţeaua locala şi doar temporar pentru eventuale teste şi verificari.
5. Trebuie sa nu transmita prin e-mail fişiere atasate despre care stiu ca pot fi infectate cu un virus
6. Nu trebuie sa deschida fişiere atasate primite de la surse nesolicitate sau care nu prezinta incredere.

18.5 Politica de internet

Aceasta politica stabileste un cadru de lucru controlat pentru furnizarea accesului la internet.

Vor fi furnizate directii, reguli de conduita şi indrumari privind utilizarea internetului şi schimbul de informaţii cu alti useri din internet fie din cadrul Institutului de Biochimie cat şi din exteriorul ei.

18.5.1 Reguli:

1. Utilizarea internetului pentru e-mail, cautari web, tranzactii de business autorizate vor fi permise pentru acei useri Institutului de Biochimie care au cerut şi au capatat autorizarea necesara.
2. Accesul la internet din interiorul Institutului de Biochimie se va face prin intermediul firewall-ului Institutului de Biochimie, alt tip de acces (modem,remote access sau contracte individuale cu ISP) nu este permis.
3. Toate fişierele downloadate din internet sunt scanate de viruşi pe firewall-ul Institutului de Biochimie iar apoi de antivirusul local de pe statia de lucru. Utilizatorii isi asuma intreaga responsabilitate dacă introduc viruşi din fişiere downloadate din surse nesigure.
4. Utilizarea bandei de internet în scopuri personale este strict interzisa.
5. Scrisorile de tip Chain (in lanţ), imagini grafice cu aspecte ofensatoare sau de tip rasial sau sexual, umorul ofensator sunt strict interzise iar utilizarea lor duce la sanctiuni.
6. Toti utilizatorii vor aborda o imagine profesionala prin e-mail.

7. Accesul din afara Institutului de Biochimie la datele de pe servere va fi facut prin VPN de către acei useri autorizati sa o faca şi anume la acele date la care au drepturi specificate. Orice alta incercare de a accesa datele poate fi considerata un acces ilegal la informaţii.

18.5.2 Anexa 1

Exemple de activităţi interzise în reţeaua Institutului de Biochimie :

- folosirea de software peer-to-peer (p2p), de exemplu: eDonkey, eMule, Kazza, DC++, ODC, bittorrent sau altele
- generarea de SPAM atât pe e-mail cât şi pe chat-uri sau alte aplicaţii
- flood (indiferent de natura acestuia), de exemplu ping flood
- răspândirea de aplicaţii de tip virus, troieni, viermi, spyware sau altele
- folosirea de aplicaţii de tip key-logere
- modificarea adresei MAC a plăcii de reţea
- utilizarea de programe pentru scanarea reţelei, exploit-uri
- realizarea de tunele
- transmiterea de mesaje cu caracter comercial
- publicitatea cu caracter comercial
- folosirea de software piratat pe calculatoarele Institutului de Biochimie sau conectate la reţeaua Institutului de Biochimie
- jocuri on-line

19 PSI 19 - Politica privind securitatea laptop-urilor

19.1 Introducere

Aceasta politică descrie controalele necesare pentru minimalizarea riscurilor de securitate informaţională care pot afecta laptopurile Institutului de Biochimie.

Toate sistemele Institutului de Biochimie se confruntă cu riscuri de securitate a informaţiilor. Laptopurile sunt instrumente cheie ale activităţii, dar însăşi portabilitatea lor le face vulnerabile în faţa daunelor fizice sau furtului. Mai mult, faptul că sunt adesea folosite în afara perimetrului Institutului de Biochimie sporeşte ameninţarea din partea oamenilor care nu lucrează pentru Institutului de Biochimie şi care pot să nu-i dorească binele.

Computerele portabile sunt vulnerabile în special faţă de avarii fizice, pierdere sau furt, fie pentru redistribuire (hoţi oportunişti), sau pentru informaţiile pe care le conţin (spioni economici).

Nu trebuie uitat că impactul acestor breşe de securitate include nu doar costul de înlocuire al echipamentului fizic, ci şi valoarea oricăror date ale Institutului de Biochimie stocate pe, sau accesibile prin acesta. Informaţia este o resursă cheie a Institutului de Biochimie. Depindem enorm de sistemele computerizate pentru obţinerea informaţiilor economice complete şi exacte când şi unde avem nevoie de ele. Impactul unui acces neautorizat la date, sau al unor modificări aduse datelor importante sau sensibile ale Institutului de Biochimie pot depăşi cu mult valoarea intrinsecă a echipamentului.

Aceasta politică face referinţă la alte politici generale de securitate a informaţiei, dar informaţiile prezentate aici sunt legate direct de laptop-uri si, în caz de conflict, au prioritate faţă de alte politici.

19.2 Controale fizice de securitate pentru laptopuri

- Securitatea fizică a laptopului revine în responsabilitatea celui căruia i-a fost încredinţat spre utilizare, astfel încât sunteţi obligaţi să luaţi toate măsurile posibile pentru evitarea riscurilor.
- Pe cât posibil, ţineţi laptopul în posesia dumneavoastră şi în raza vizuală, ca şi cum ar fi portofelul, geanta sau telefonul mobil. Fiţi extrem de atenţi în locurile publice, ca aeroporturi, staţii de cale ferată sau restaurante. Hoţii au nevoie doar de o fracţiune de secundă pentru a fura un laptop nesupravegheat.
- Încuiaţi laptopul astfel încât să nu fie la vedere când nu-l folosiţi, de preferat într-un dulap sau raft sau seif solid. Acest lucru este valabil acasă, la birou sau la hotel. Niciodată nu lăsaţi un laptop nesupravegheat în maşina. Dacă este absolut necesar, ascundeţi-l în portbagaj sau în torpedo, dar în general este mai sigur să îl luaţi cu dumneavoastră.
- Transportaţi şi depozitaţi laptopul într-o geanta specială de laptop sau într-o servietă mai rezistentă, pentru a reduce riscul de lovire accidentală. Nu-l scapaţi şi nu-l izbiţi! Ambalajul de protecţie cu bule de aer poate fi folositor. O servietă cu aspect comun va atrage mai puţin atenţia hoţilor decât o geantă de laptop evidentă.
- Notaţi undeva marca, modelul, numărul de serie, eticheta Institutului de Biochimie de proprietate asupra laptopului, dar nu ţineţi aceste informaţii în acelaşi loc cu laptopul. Dacă acesta a fost pierdut sau furat, anunţaţi imediat Poliţia, şi informaţi Responsabilul IT cât mai curând posibil, în interval de câteva ore, nu câteva zile.

19.3 Protecţia laptopurilor în faţa viruşilor

- Viruşii reprezintă o ameninţare majoră la adresa Institutului de Biochimie, iar laptopurile sunt în special vulnerabile dacă antivirusul nu este la zi. Antivirusul TREBUIE updatat cel puţin lunar. Acest lucru este cel mai simplu de realizat prin conectarea la reţeaua Institutului de Biochimie pentru a rula procesul automat de updatare. Dacă, din diferite motive, nu vă puteţi conecta, contactaţi Responsabilul Asistenţă IT pentru consultanţă legat de obţinerea şi instalarea update-urilor pentru antivirus.
- Ataşamentele la email-uri au ajuns principala sursă pentru viruşi de calculator. Evitaţi deschiderea oricărui ataşament dacă nu vă aşteptaţi să-l primiţi de la acea persoană.
- Întotdeauna scanaţi orice fişier adus pe computerul dumneavoastră, din orice sursă (CD, DVD, harddisk-uri externe sau memorii USB, fişiere din reţea, ataşamente e-mail sau fişiere de pe internet). De obicei scanarea de viruşi se produce automat, dar Responsabilul Asistenţă IT va poate cere să porniţi o scanare manuală dacă vreţi să fiţi siguri.
- Raportati imediat orice incident de securitate (cum ar fi infecţii cu viruşi) către Responsabilul IT, pentru a limita pagubele.
- Răspundeţi imediat oricărui mesaj de atenţionare legat de descoperirea unui virus pe calculatorul dumneavoastră, sau dacă suspectaţi că aţi fost infectat cu un virus (de exemplu, activităţi neobişnuite asupra fişierelor) contactând Responsabilul Asistenţă IT. Nu trimiteţi nici un fişier şi nu uploadaţi date în reţea dacă suspectaţi că sunteţi infectat.
- Acordaţi atenţie suplimentară scanării de viruşi a sistemului înainte de a trimite fişiere în afara Institutului de Biochimie. Aici sunt incluse email-urile şi CD-urile pe care le creaţi.

19.4 Controale împotriva accesului neautorizat la datele de pe laptopuri

- Trebuie să folosiţi software-ul de encriptare autorizat pe toate laptopurile Institutului de Biochimie, trebuie să folosiţi o parolă/frază de encriptare lungă şi puternică, pe care să o păstrati bine. Contactaţi Departametul de Asistenţă IT pentru mai multe informaţii legate de encriptarea datelor de pe laptop. Dacă laptopul este pierdut sau furat, encriptarea oferă protecţie extrem de puternică împotriva accesării neautorizate a datelor.
- Sunteţi personal răspunzator pentru toate accesările la reţea şi la alte sisteme realizate folosind numele dumneavoastră de utilizator, deci păstraţi parola ca secret absolut. Niciodată nu o impărtaşiţi cuiva, nici măcar cu familia, prietenii.
- Laptopurile Institutului de Biochimie sunt furnizate pentru utilizare oficială de către angajatii autorizaţi. Nu imprumutaţi laptopul sau permiteţi să fie folosit de alţii, cum ar fi familia sau prietenii.
- Evitati sa lasati laptopul nesupravegheat şi logat. Intotdeauna inchideti, delogati sau activati un screensaver parolat inainte de a pleca de langa laptop.

19.5 Alte controale pentru laptopuri

19.5.1 Software neautorizat

Nu descarcaţi, instalaţi sau utilizaţi software neautorizat. Acesta poate introduce vulnerabilităţi de securitate grave în reţeaua Institutului de Biochimie , simultan cu afectarea laptopului. Programe care permit accesarea calculatorului de la distanţă (exemplu: PCAnywhere), şi aşa-numitele “hacking tools” (exemplu: sniffere şi

programe de spart parole) sunt interzise expres pe echipamentele Institutului de Biochimie, cu expresia acelora care au fost pre-autorizate explicit de către management pentru scopuri legitime.

19.5.2 Software nelicenţiat

Fiti atenţi la licenţe. Majoritatea programelor, cu excepţia celor identificate ca “freeware” sau “program public”, pot fi instalate şi/sau folosite doar dacă a fost achitată o taxă de licenţiere. Programele shareware sau trial trebuie şterse sau licenţiate până la sfârşitul perioadei permise. Unele programe au utilizarea gratuită limitată la persoane fizice, în timp ce utilizarea comercială necesită o taxă. Indivizii şi companiile sunt urmăriţi pentru încălcarea legii copyright-ului; nu riscaţi ca dumneavoastră şi Institutului de Biochimie să sufere prin încălcarea legii.

19.6 Copii de siguranţă

Spre deosebire de PC-uri, cărora li se face backup automat, trebuie să vă faceţi propriile copii de siguranţă la datele de pe laptop. Cel mai simplu mod de a face acest lucru este să vă conectaţi la reţea şi să vă upload-aţi regulat datele — ideal ar fi zilnic, dar măcăr saptămânal. Dacă nu puteţi accesa reţeaua, este responsabilitatea dumneavoastră să faceţi copii regulate ale datelor pe CD/DVD, memorii USB, etc. Asigurati-vă că aceste back-upuri offline sunt encriptate şi securizate fizic. Tineţi minte, dacă laptopul este furat, pierdut sau avariat, sau pur şi simplu nu mai funcţionează, poate fi imposibil să recuperaţi vreo informaţie de pe laptop. Copiile de siguranţă vă pot salva multe ore de muncă suplimentară.

19.7 Legi, reglementări şi politici

Trebuie să respectaţi legile, reglementările şi politicile din domeniul utilizării computerelor şi informaţiilor. Licenţele pentru programe au fost deja amintite, iar legile legate de intimitatea informaţională sunt un alt exemplu. Diferite politici la nivel de organizaţie se aplică la laptopuri, datele pe care le conţin, şi accesul la reţea (inclusiv utilizarea internetului).

19.7.1 Materiale nepotrivite

Conducerea Institutului de Biochimie nu va tolera materiale nepotrivite, cum ar fi materialele pornografice, rasiste, defăimătoare sau de hărţuire, imagini, filme sau email-uri care pot ofensa sau jena. Niciodată nu stocaţi, copiaţi sau puneţi în circulaţie astfel de materiale pe laptop şi evitaţi site-urile dubioase. Responsabilul IT monitorizează reţeaua şi sistemele pentru astfel de materiale şi jurnalizează folosirea internetului; ei vor raporta pe cei care încalcă grav/repetat aceste instrucţiuni, precum şi materialele ilegale direct angajatilor, şi procesul disciplinar va fi iniţiat. Dacă aţi primit astfel de materiale prin email sau alte mijloace, ştergeţi-le imediat. Dacă aţi ajuns din greşeală pe un site ofensator, daţi “Back” imediat sau închideţi browserul. Dacă primiţi spam-uri constant, apelaţi la Responsabilul Asistenţă IT.

19.7.2 Aspecte ce ţin de sănătatea sau siguranţa angajaţilor

În mod normal laptopurile au tastaturi, display-uri şi alte dispozitive care sunt mai puţin confortabil de utilizat ca cele de pe desktop-uri, sporind şansele de a vă răni. Folosirea laptopului de pe genunchi nu este indicată! Reduceţi timpul petrecut în fata laptopului. De câte ori este posibil, puneţi laptopul pe o masă şi staţi confortabil pe un scaun. Dacă folosiţi laptopul la birou, sunteţi încurajaţi să achizitionaţi un dispozitiv de genul “docking station” şi o tastatură de dimensiuni normale, un mouse normal şi un ecran postat întotdeauna la înălţimea corectă. Opriţi-vă din utilizarea laptopului şi solicitaţi consultaţie din partea medicul de medicina muncii dacă suferiţi de simptome de genul durerilor de încheieturi, presiune în ochi sau dureri de cap, simptome pe care le banuiţi cauzate de lucru la laptop.