SECURIZAREA INFORMAŢIILOR

COD: I-SICD-01

INSTRUCTIUNE

RECTOR,
Prof. univ. dr. ing. Valentin NEDEFF

	Prenumele şi numele	Semnătura
Departamentul de Management	**Conf. univ. dr. ing. Mirela PANAINTE-LEHĂDUȘ**	
Avizat	**Ing. Ciprian Ioan Drugă**	
Elaborat	**Marcel Olatuc**	

EDIŢIA: 1 **REVIZIA: 0 1 2 3 4 5** **EXEMPLAR NR.:**

Intră în vigoare începând cu data de 27.03.2014, prin aprobarea în Ședința Consiliului de Administrație al Universității ”VASILE ALECSANDRI” din Bacău.

1. SCOP

Prezenta instructiune stabileste normele de practică privind asigurarea securităţii informaţiei electronice. Securizarea se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul Universităţii "Vasile Alecsandri" din Bacău, sunt proprietatea Universităţii în condiţiile legilor în vigoare.

2. DOMENIUL DE APLICARE

Se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii. Următoarele entităţi şi utilizatori sunt vizaţi în mod distinct de prevederile instrucţiunii:

- Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- Colaboratorii Universităţii "Vasile Alecsandri" din Bacău care au acces la sistem;
- Furnizorii Universităţii " Vasile Alecsandri" din Bacău care au acces la sistem;
- Studenţii Universităţii " Vasile Alecsandri" din Bacău;
- Alte persoane, entităţi sau organizaţii care au acces la sistem.

3. DOCUMENTE DE REFERINTĂ

- Regulamentul privind utilizarea sistemului informatic al Universităţii "Vasile Alecsandri" din Bacău - R-12.05.01 E1R1;
- Regulamentul de organizare şi funcţionare a Serviciului informatizare şi comunicaţii digitale - R-12.05.02 E1 R0.

4. DESCRIERE

4.1. Securizarea datelor se face atât din punct de vedere fizic cât şi logic.

4.2. Securitatea fizică a unui sistem informatic constă in asigurarea securităţii componentelor hardware a unui sistem informatic şi anume protejarea împotriva furtului sau vandalizării acestora prin plasarea lor într-o încăpere sigură. De asemenea, trebuie asigurată paza şi accesul persoanelor străine. O alta securitate fizică care trebuie avută în vedere este securitatea care are ca obiect copiile datelor şi programelor salvate (backup). Aceste copii trebuie protejate împotriva furtului, vandalizării lor. Pe lângă securitatea fizică este necesară şi asigurarea securităţii logice. Pentru a avea efectul scontat acestea trebuie să existe concomitent. Având în vedere că un sistem informatic conţine pe lângă date şi o serie de servicii şi mai multe tipuri de acces din punct de vedere al securităţii logice. Responsabili pentru securitatea datelor sunt membrii serviciului SICD.

4.3. Informaţiile electronice supuse regimului de securitate sunt:

1. conţinutul bazelor de date;
2. conturile poştale – denumire şi conţinut;
3. informaţii financiare de uz intern;
4. fişiere stocate pe calculatoarele universităţii, de uz personal;
5. fişierele de configurare ale serviciilor intra şi internet;
6. copiile de siguranţă şi arhivele electronice.

4.4. Securizarea informaţiilor electronice în cadrul Universităţii se implementează pe două nivele:
- nivelul fizic;
- nivelul logic.

4.5. Nivelul fizic de securizare a informaţiilor digitale implică:
1. amplasarea serverelor de date şi a echipamentelor de comunicaţie critice în locaţii izolate, dotate cu minim 2 încuietori, supraveghere video şi sisteme de alarmă pentru incendiu;
2. toate echipamentele de stocare a datelor sunt prevăzute cu surse neîntreruptibile de alimentare, cu autonomie de minim 2 ore;
3. accesul fizic la serverele de date şi echipamentele de comunicaţie critice se face numai de către personalul autorizat SICD;
4. fiecare intervenţie fizică la serverele de date este înregistrată într-un jurnal care conţine data şi ora accesului, operaţiile efectuate, data şi ora plecării;
5. staţiile de lucru ale personalului universităţii sunt amplasate în încăperi dotate minim cu încuietoare, şi dispuse astfel încât să nu permită vizualizarea facilă a ecranului de către alte persoane.

4.6. Nivelul logic de securizare a informaţiilor digitale implică:
1. fiecare staţie de lucru şi / sau server de date / echipament de stocare date / echipament de comunicaţie sunt protejate prin parolă;
2. în cazul staţiilor de lucru ale personalului universităţii, gestiunea parolelor de acces la computer cade în sarcina utilizatorului, acesta fiind singurul care răspunde pentru integritatea şi securitatea informaţiilor stocate pe calculatorul său;
3. în cazul serverelor şi a echipamentelor de comunicaţie, gestiunea parolelor de acces cade în sarcina SICD;
4. parolele de acces sunt informaţii care nu se divulgă terţilor (inclusiv rudelor de gradul I);
5. conturile poştale sunt gestionate de către SICD, la nivel centralizat, accesul la conturi fiind permis pe bază de user şi parolă transmise fiecărui utilizator, personal;
6. conţinutul conturilor poştale este scanat la nivel de server cu programe anivirus şi sunt protejate la acces străin prin programe de monitorizare şi detecţie a intruziunilor (IDS);
7. bazele de date sunt protejate prin parole de acces şi prin efectuarea de copii de siguranţă la intervale cuprinse între 24 de ore şi 7 zile;
8. sistemele de operare tip server, precum şi echipamentele de comunicaţie critice (routere, switch-uri) sunt protejate prin parole de acces având lungimea minimă de 10 caractere, schimbate periodic la interval de 14 zile;
9. serverele de date sunt protejate prin firewall şi sunt monitorizate permanent pentru sesizarea oricăror disfuncţionalităţi. Monitorizarea se face atât manual, prin consultarea zilnică a jurnalelor (loguri), cât şi automatizat, prin emiterea de e-mailuri şi/sau SMS-uri atunci când un serviciu de date îşi întrerupe activitatea;
10. toate căile de acces Internet (gateways) sunt prevăzute cu firewall incluziv.