Ministerul Educației Naționale
Universitatea Europeană "Drăgan" din Lugoj
305500 Lugoj, jud. Timiș
str. Ion Huniade nr. 2
tel. 0256 359 198, fax: 0256 359 198
e-mail: ued@deu.ro
www.universitateaeuropeanadragan.ro

Universitatea Europeana Dragan

PROCEDURI PRIVIND SECURITATEA INFORMAȚIILOR ȘI A SISTEMULUI IT DIN CADRUL UNIVERSITĂȚII EUROPENE "DRĂGAN" DIN LUGOJ

Cod procedură: UED P0.03/DS

Elaborat:	*Prorector* Conf. univ. dr. Gabriel Ionel Dobrin	
Avizat:	*Rector* Conf. univ. dr. Dumitru Cornean	
Aprobat:	*Senatul UED*	HS nr. 25 din 15.04.2019
	Președinte Senatul Universitar Conf. univ. dr. Sorin Blaj	

Ediția: 1

Revizia: 0

Intrat în vigoare la data de: 15.04.2019

1. SCOP

Procedura stabileşte politicile, principiile şi modalităţile de acţiune privind asigurarea securităţii informaţiilor şi a sistemului IT din cadrul UED.

2. DOMENIU DE APLICARE

Procedura se aplică de către Administratorul Rețele Informatice (ARI) din cadrul Universității, acesta fiind înlocuit momentan de către o firmă de consultanță din domeniul IT, care se ocupă de toate aceste aspecte.

3. DEFINIȚII ȘI ABREVIERI

3.1. Definiții

Virus informatic - Un program care se ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte deranjante sau distructive.

Vierme informatic - Un program care se auto-copiază în spaţiul de stocare al unui sistem informatic şi care se răspândeşte către alte calculatoare prin intermediul reţelei.

Cal troian – Este obicei un virus informatic sau un vierme informatic care este disimulat sub forma unui program atractiv sau inofensiv.

Phishing – un atac de *phising* are loc atunci când se încearcă inducerea în eroare a unui utilizator astfel încât acesta să furnizeze online informaţii de identificare sau cu caracter personal.

Incident de securitate - În termeni informatici este definit ca fiind un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic.

Vulnerabilitatea sistemului informatic - Slăbiciune care poate fi exploatată în scopul accesării neautorizate a resurselor sau informaţiilor.

Atac informatic - Încercarea de a exploata vulnerabilitatea unui sistem informatic.

Control de securitate - Măsură de gestionare vulnerabilităţii sistemului informatic, în scopul reducerii expunerii la riscuri.

3.2. Abrevieri

UED = Universitatea Europeană "Drăgan" din Lugoj

ARI = Administrator Rețele Informatice

DS = Domeniul specific procedurii

4. DOCUMENTE DE REFERINȚĂ

"**1.** Legea nr. 8/1996 - privind dreptul de autor şi drepturile conexe, cu modificările şi completările ulterioare;

2. Legea nr. 455/2001 - privind semnătura electronică, cu modificările şi completările ulterioare;

3. Legea nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările şi completările ulterioare;

4. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)"[1].

5. DESCRIEREA PROCESULUI

5.1. PRINCIPIILE FUNDAMENTALE PRIVIND ASIGURAREA SECURITĂȚII INFORMAȚIONALE ȘI A SISTEMULUI IT

Principiile care trebuie îndeplinite pentru a asigura securitatea informațională și a sistemului IT din cadrul UED sunt:

I. Principiul responsabilităţii. Responsabilităţile legate de securitatea informațională și a sistemului IT pentru deţinătorii, furnizorii şi utilizatorii de sisteme informatice ori servicii de date trebuie să fie clare, concise și explicite.

II. Principiul conştientizării. Pentru a asigura securitatea informațională și a sistemului IT, deţinătorii, furnizorii şi utilizatorii acestora trebuie să poată accesa şi dobândi cunoştinţele necesare, să fie informaţi despre existenţa şi cadrul general al măsurilor, practicilor şi procedurilor de securitate implementate pentru diminuarea riscurilor.

III. Principiul eticii. Sistemele informatice şi securitatea informațională trebuie folosite într-o manieră în care drepturile şi interesele legale ale celorlalţi să nu fie afectate.

IV. Principiul multidisciplinarităţii. Măsurile, practicile şi procedurile de asigurare a securităţii sistemelor informatice trebuie să ţină cont de toate consideraţiile, aspectele relevante şi cele legale.

V. Principiul proporţionalităţii. Nivelurile de securitate, costurile, măsurile, practicile şi procedurile trebuie să fie corespunzător dimensionate şi proporţionale cu valoarea şi gradul de încredere necesar pentru fiecare tip de informaţie.

VI. Principiul integrării. Măsurile, practicile şi procedeele de asigurare a securităţii sistemelor informatice din cadrul UED trebuie să fie coordonate instituţional şi integrate într-un sistem global de securitate informațională.

VII. Principiul actualităţii. Compartimentele funcționale ale Universității, indiferent de tipul lor, trebuie să acţioneze rapid şi într-o manieră coordonată pentru a preveni şi a răspunde eficient la apariţia breşelor de securitate.

[1] Legislație specifică

VIII. Principiul reevaluării. Securitatea sistemelor informatice trebuie analizată şi reevaluată periodic pentru a se putea răspunde în timp util celor mai noi tipuri de agresiuni informatice.

5.2. POLITICA DE ASIGURARE A SECURITĂȚII RESURSELOR INFORMATICE

Politica de asigurare a securității resurselor informatice are ca scop fundamental asigurarea integrităţii, confidenţialităţii şi a disponibilităţii informaţiei.

1. Confidenţialitatea 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 UED, reprezintă proprietatea Universității.

Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la resursele informatice.

2. Integritatea se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcţionarea optimă a întregului sistem IT din cadrul UED.

3. Politica de securitate are astfel ca scop și stabilirea cadrului general necesar pentru elaborarea și implementarea procedurilor de securitate, acestea fiind obligatorii pentru toţi utilizatorii resurselor informatice.

5.3. POLITICA DE SECURITATE ÎN UTILIZAREA RESURSELOR INFORMATICE

Scopul elaborării politicii de securitate specifice utilizării resurselor informatice îl reprezintă crearea cadrului necesar în vederea elaborării procedurilor de securitate.

Implementarea acestei politici se face prin intermediul unor reguli de bază și a unor măsuri generale menite să asigure securitatea informațiilor din UED, ele fiind obligatorii pentru toți utilizatorii resurselor informatice ale Universității.

Principalele reguli din cadrul UED privind utilizarea corectă a resurselor informatice sunt:

1) Utilizatorii trebuie să înștiințeze de urgență ARI, în cazul în care se constată o problemă ori o posibilă breșă de securitate în sistemul IT al Universității.
2) Acțiunile utilizatorilor nu trebuie să compromită parțial ori total, deliberat sau accidental, confidențialitatea, integritatea și disponibilitatea informațiilor.
3) Utilizatorii vor obține acces la date sau programe cu consimțământul expres al ARI, în situație contrară accesul acestora nefiind permis.
4) Nu vor fi divulgate și nici înstrăinate datele de autentificare proprii atunci când utilizatorii se vor loga în rețeaua UED (parole, nume utilizator, conturi etc.).
5) Nu va fi permisă realizarea de copii neautorizate de către utilizatori.
6) Nu va fi permisă distribuirea de materiale protejate în conformitate cu legile privind copyright-ul.
7) Utilizarea programelor de tip shareware ori freeware se va face doar cu consimțământul expres al ARI și doar în situația în care, acest lucru este absolut necesar.

8) Descărcarea, instalarea și rularea de programe care pun în pericol sistemul IT al UED este strict interzisă.
9) Utilizatorii nu se pot angaja să utilizeze resursele informatice ale Universității împotriva intereselor de orice fel ale entității.
10) Administrarea, întreținerea și dezvoltarea sistemul IT al UED îi revine ARI
11) Ansamblul echipamentelor conectate la rețeaua UED vor fi configurate de către ARI în conformitate cu specificațiile acestora.
12) În nici un fel, utilizatorii nu vor putea interveni fie în mod direct, fie în mod indirect, în structura sistemului IT al Universității.

Monitorizarea sistemului IT al UED se va face astfel încât să fie posibilă detectarea în cel mai scurt timp posibil a tuturor atacurilor informatice, precum și a posibilelor situații de încălcare a protocoalelor de securitate.

Activitățile utilizatorilor ce utilizează sistemul IT din cadrul UED pot fi înregistrate și analizate, cu respectarea strictă a criteriilor de confidențialitate instituțională și personală.

Un server poate fi conectat la sistemul IT al Universității, după ce, în prealabil, acesta a fost securizat în mod corespunzător.

Parolele de acces utilizate pentru accesarea sistemului IT al UED trebuie să îndeplinească o serie de condiții obligatorii de securitate, și anume:

- schimbarea parolelor în mod regulat;
- lungimea parolelor să fie cât mai mare;
- diversitatea adecvată și numărul de caractere utilizate care să fie cât mai mare;
- complexitatea parolelor;
- este interzisă reutilizarea parolelor vechi și a celor foarte simple;
- în situația stocării parolelor de către ARI, acestea vor trebui să fie securizate;
- utilizatorii de conturi din sistemul IT al Universității nu pot divulga către terți sub nicio formă, informațiile de acces în rețeaua UED, inclusiv parolele acestora;
- dacă există suspiciuni asupra unei parole în ceea ce privește divulgarea sa, atunci aceasta va fi schimbată de urgență;
- este interzis ca utilizatorii să folosească software specializat de stocare a parolelor.

În ceea ce privește Sistemul de mesagerie electronică, Skype for Business, utilizat în cadrul UED, următoarele activități sunt strict interzise:

- trimiterea mesajelor de intimidare ori hărțuire;
- utilizarea Sistemului de mesagerie electronică, în cu totul alte scopuri, altele decât cele profesionale;
- distribuirea neautorizată a materialelor protejate prin legea copyright-ului;
- utilizarea unei identități false și a programelor de poștă electronică neautorizate de către ARI.

Măsurile de informare și de instruire, cu privire la angajații UED, pot fi făcute la angajare, periodic sau ori de câte ori acest lucru este necesar. Vor fi comunicate și ansamblul modificărilor realizate în structura procedurilor de securitate ale instituției.

Angajații UED trebuie să fie informați și să cunoască în mod real, care sunt amenințările și riscurile generate de utilizările defectuoase ale sistemului IT.

5.4. REGULI DE BAZĂ ȘI MĂSURI GENERALE PRIVIND SECURITATEA INFORMAȚIILOR ȘI A SISTEMULUI IT DIN CADRUL UED LUGOJ

Utilizatorii sistemului IT din cadrul UED trebuie în mod obligatoriu să respecte următoarele reguli de bază:

1. Utilizatorii rețelei informatice a UED împreună cu ARI vor trebui să salveze periodic toate datele importante cu care aceștia lucrează: documente, baze de date etc., pe un suport extern (HDD extern), care va fi păstrat în deplină siguranță de către ARI.
2. Utilizatorii vor fi instruiți de către ARI cu privire la utilizarea în condiții de siguranță deplină a unității PC pe care aceștia lucrează, precum și în ceea ce privește deprinderea modalităților primare privind salvarea periodică a tuturor datelor importante.
3. Utilizatorii vor urmări în mod sistematic actualizările periodice ale sistemului de operare instalat, ale programului antivirus, precum și actualizările periodice ale tuturor programelor software instalate pe stația de lucru; dacă toate aceste actualizări nu pot fi efectuate, atunci va fi informat de urgență ARI al UED, pentru a determina cauza și pentru a remedia ansamblul deficiențelor constatate.
4. Utilizatorii nu pot instala pe stațiile de lucru programe neautorizate, programe fără licență ori software care nu are nicio legătură cu activitatea profesională derulată în cadrul UED.
5. Utilizatorii vor utiliza pentru transmiterea ori primirea de mesaje electronice de serviciu doar adresele de email instituționale.
6. Utilizatorii vor investiga în mod formal, atunci când acest lucru este posibil, autenticitatea mesajelor email provenite din surse îndoielnice, pentru a nu periclita securitatea sistemului IT al UED.
7. Utilizatorii vor evita deschiderea fișierelor atașate suspecte din cadrul email-urilor provenite din surse îndoielnice, evitându-se în acest fel compromiterea securității rețelei UED.
8. Pe cât posibil, se va evita folosirea memoriilor externe de tip flash (USB) pentru a se diminua posibilitatea expunerii la risc a sistemului IT al UED.

Măsurile generale privind securitatea informațiilor și a sistemului IT al UED se referă în mod direct la:

1. Utilizarea de surse de alimentare neîntreruptibile pentru asigurarea unei alimentări sigure a echipamentelor.
2. Efectuarea de verificări periodice ale sistemului IT al UED.
3. Efectuarea de revizii periodice ale sistemului IT al UED.

4. Interzicerea utilizării de software neautorizat.
5. Folosirea parolelor sigure ca și complexitate.
6. Schimbarea periodică a parolelor.
7. Verificarea periodică a stațiilor de lucru din cadrul UED cu ajutorul programelor antivirus și actualizarea permanentă a definițiilor privind virușii.
8. Identificarea rapidă a vulnerabilităților ce afectează securitatea sistemului IT al UED.
9. Verificarea periodică a securității sistemului IT al UED de către ARI.
10. Gestionarea corectă a copiilor de rezervă de tip backup în ceea ce privește confidențialitatea, integritatea, disponibilitatea și securitatea acestora.

6. RESPONSABILITĂȚI ȘI COMPETENȚE

Responsabilitățile și competențele principale ale ARI sunt:

1. Crearea ansamblului condițiilor de aplicare a procedurilor privind securitatea informațiilor și a sistemului IT din cadrul UED Lugoj.
2. Monitorizarea permanentă a nivelului de securitate al sistemului IT.
3. Răspunde de configurarea rețelei informatice în conformitate cu politica de securitate IT.
4. Intervenția operativă pentru rezolvarea problemelor apărute în rețeaua informatică a UED.
5. Instruirea utilizatorilor în ceea ce privește accesul la/și utilizarea resurselor informatice.
6. Stabilirea resurselor (hardware, software, licențe și servicii) necesare funcționării în bune condiții a rețelei informatice.
7. Definirea și implementarea politicilor și procedurilor referitoare la funcționarea rețelei informatice: politica de securitate, procedura de creare/administrare/ștergere a conturilor utilizatorilor, procedura de salvare (backup) și restaurare a datelor, planul de recuperare în caz de dezastru.
8. Propunerea măsurilor de optimizare în ceea ce privește sistemul IT al UED.
9. Asigurarea întreținerii echipamentelor hardware.
10. Suport de utilizatori – Helpdesk.
11. Managementul conturilor – Account management.
12. Actualizarea software-ului existent.
13. Implementarea de noi soluții software.
14. Upgrade hardware.
15. Securitatea datelor – GDPR compliance.
16. Troubleshooting.

7. APROBAREA PROCEDURILOR ȘI INTRAREA ACESTORA ÎN VIGOARE

Aprobarea procedurilor privind securitatea informațiilor și a sistemului IT din cadrul UED Lugoj este de competenţa Senatului UED.

Intrarea în vigoare a prezentelor proceduri are loc la data aprobării acestora în Senatul UED.