M U Z E U L J U D E Ţ E A N B O T O Ş A N I
Unirii, 15, 710221– Botoşani, România
tel: 0231/51.34.46; fax: 0231/53.69.89,
e-mail: istorie@muzeubt.ro
Nr. _____ din _____

Aprob,
Manager,
Aurel Melniciuc

Notă de serviciu

Având în vedere Regulamentul (UE) 679/2016 al Parlamentului European și al Consiliului 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), începând cu 30.05.2018 intră în vigoare Regulamentul intern de Securitate IT, atașat la prezenta Notă de serviciu.

Șefii de secții vor asigura:

- Comunicarea către salariați a Regulamentului;
- Accesul reprezentantului firmei de service la computerele avute în gestiune de salariați în vederea implementarea politicilor de securitate prezentate în Regulament;
- Fișele de înscriere, parteneriatele, contractele sau alte materiale folosite pentru activitățile muzeale și educative vor avea înscrise obligatoriu textele: ”În conformitate cu Regulamentul European 2016/*679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date*, vă dați consimțământul pentru prelucrarea datelor cu caracter personal, a fotografiilor și filmărilor realizate pe parcursul desfășurării evenimentului, numai pentru următoarele scopuri: organizarea, desfășurarea și promovarea eveenimentului”; ”Sunt de acord ca datele personale să fie utilizate pentru informarea privind organizarea viitoarelor evenimente la Muzeul Județean Botoșani.

Regulament intern Securitate IT

Vă informăm că, începând cu data de 25 mai 2018, sunt aplicabile prevederile Regulamentului (UE) nr. 679/2016 al Parlamentului European și al Consiliului Uniunii Europene, 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).

Drept pentru care conform regulamentului sunt absolut necesare o serie de măsuri tehnice de securitate și protecție a datelor din sistemul informatic al instituției.

Implementarea securității într-o rețea de calculatoare cuprinde trei aspecte importante: **confidențialitatea, integritatea și disponibilitatea**.

Confidențialitatea reprezintă calitatea unei rețele de a asigura accesul la informație doar persoanelor autorizate.

Integritatea garantează faptul că informația nu a fost modificată de persoane neautorizate.

Disponibilitatea poate fi definită ca timpul în care rețeaua de calculatoare și resursele din cadrul ei sunt operaționale.

Pentru fiecare din aceste aspecte ale securității rețelelor de calculatoare există atacuri, astfel încât securizarea unei rețele de calculatoare trebuie să implementeze fiecare din aceste aspecte.

Măsuri de prevenție:

- Identificarea, autorizarea și monitorizarea activității utilizatorilor;
- Securizarea perimetrului rețelelor;
- Asigurarea confidențialității și integrității datelor;
- Monitorizarea rețelei;
- Managementul echipamentelor și infrastructurii de securitate.

Tipuri de atacuri și vulnerabilități

Există două cauze majore ce pot constitui amenințări pentru o rețea de calculatoare, chiar după ce a fost implementată o politică de securitate corectă:

- Vulnerabilități (probleme cauzate de tehnologie)
- Configurare necorespunzătoare.

Vulnerabilitățile sunt probleme ale sistelelor de operare, protocoalelor TCP/IP, dispozitivelor de rețea prin care un atacator poate accesa rețeaua fără a respecta politica de securitate implementată.

Chiar dacă vulnerabilitățile sunt problemele cele mai grave și mai greu de controlat, trebuie însă notat că cele mai multe probleme apar datorită configurării incorecte sau definirii unei politici de securitate necorespunzătoare.

Atacurile asupra unei rețele de calculatoare pot fi clasificate în:

- Atacuri interne sau externe și
- Atacuri structurate sau nestructurate.

Atacurile esterne sunt efectuate din afara organizației (din punctul de vedere al rețelei).

Atacurile interne sunt efectuate din rețeaua organizației.

Atacurile nestructurate sunt atacurile care sunt inițiate de indivizi neexperimentați ce utilizează exploit-uri disponibile pe Internet. Exploit-urile sunt programe ce exploatează vulnerabilitățile pentru a ocoli politica de securitate implementată într-o rețea.

Atacurile structurate sunt inițiate de indivizi mult mai bine motivați și cu ccunoștințe tehnice competente. Acești indivizi cunosc vulnerabilitățile de sistem și le pot folosi pentru a căpăta acces în rețea, pot detecta noi vulnerabilități de sistem și pot dezvolta cod și scripturi pentru a le exploata.

Documentul are rolul de a face angajații instituției conștienți de valoarea și semnificația informațiilor vehiculate, precum și de a familiariza utilizatorii cu metode de protecție și securitate pentru asigurarea confidențialității, integrității și disponibilității informației.

Astfel, sunt impuse o serie de reglementări care să guverneze activitatea curentă în scopul asigurării securității și integrității datelor.

De asemenea documentul conturează metodele acceptabile de utilizare a resurselor informatice vehiculate în cadrul sistemului.

Resursele informaționale vor fi utilizate într-o manieră aprobată, etică și în conformitate cu prevederile legale pentru a evita pierderea sau deteriorarea datelor.

Domeniul de aplicabilitate

Prevederile acestei politici se aplică întregului personal care are sau este responsabil cu orice acces la sistemul informatic și rețelei de calculatoare al instituției.

Asigurarea conformității

Utilizarea informațiilor presupune consimțământul utilizatorilor pentru ca instituția să monitorizeze, să inspecteze, să auditeze, să colecteze și să șteargă orice informație fără a cere permisiune și fără o notificare în prealabil.

Orice abatere de la regulamentul de securitate IT reprezintă o încălcare a prevederilor de securitate și personalul implicat va fi considerat responsabil, existând posibilitatea de a fi supus unor acțiuni disciplinare sau urmăririi penale.

Manevrarea datelor și a informațiilor

- Utilizarea sistemelor IT trebuie să fie în conformitate cu prevederile legale în vigoare;
- Este strict interzisă distribuirea documentelor interne sau a informațiilor clasificate drept confidențiale către persoane neautorizate;
- Fiecare angajat din cadrul instituției trebuie să fie conștient de riscurile și pericolele aferente ingineriei sociale.

Utilizarea și configurarea echipamentelor hardware și a aplicațiilor aferente

- Este permisă utilizarea exclusiv a softwarw-ului licențiat instalat de către responbsabilul IT sau firma de service contractată;
- Este interzisă instalarea de aplicații private sau de aplicații care încalcă drepturile de autor pe orice sistem IT;
- Toate achiizițiile de software trebuie realizate prin responsabilul IT a instituției;

Licențele Software și echipamentele hardware

Toate echipamentele hardware și aplicațiile standard cerute în scopul desfășurării activității sunt alese și achiziționate la cerere de către responsabilul IT și:

- Orice modificare neautorizată la nivelul aplicațiilor, respectiv al echipamentelor utilizate este interzisă;
- Trebuie verificate toate resursele de informații (CD-uri, atașamente la mail-uri, stick-uri USB) de cod malițios instalat (viruși, viermi, cal troian) cu un program antivirus;
- Este strict interzisă utilizarea sistemelor IT, a aplicațiilor și a datelor aferente în scopuri nelucrative diferite de scopul activității desfășurate;
- Utilizatorul echipamentelor IT din dotare este direct responsabil de integritatea fizică a acestora;
- Echipamentele trebuie tratate corespunzător, se interzice orice fel de bruscare a echipamentelor IT;
- Se interzice orice fel de intervenție în interiorul echipamentelor IT de către personal neautorizat;

- Folosirea computerelor și altor echipamente IT conectate la rețeaua internă este strict de competența angajaților proprii. Se interzice persoanelor străine folosirea oricărui echipament sau computer IT fără aprobarea conducătorului instituției.

Accesul la informații

- Informațiile și mijloacele de autentificare în sistem sunt proprietatea personală a fiecărui angajat;

  Utilizatorul este singurul responsabil cu prevenirea oricărei divulgări a acestor informații și nu este permisă utilizarea credențialelor altui angajat.
- Fiecare angajat este responsabil cu menținerea securității fiecărei informații considerate confidențială și se asigură că aceasta este protejată de acces neautorizat (vizualizare, alterare, furt sau distrugere);
- Dezvăluirea de informații clasificate drept confidențiale este strict interzisă;
- Este interzis furtul de informații de rice natură;
- Exploatarea restrselor informatice trebuie să se realizeze fără încălcarea drepturilor de autor.

Accesul la sistem

- Accesul utilizatorilor la bazele de date se va face doar de către personalul autorizat în acest sens în funcție de fișa postului;
- Salvarea parolelor este strict interzisă; de asemenea notarea sau stocarea parolelor pe orice suport fizic la vedere este strict interzisă;
- Sistemul trebuie blocat ori de câte ori angajatul părăsește biroul sau nu își utilizează calculatorul;

În cazul în care utilizatorul nu este disponibil este recomandată deconectarea de la aplicație și din sistem. Calculatorul se va bloca după 5 minute de neutilizare.

- După terminarea programului, calculatorul trebuie închis. De asemenea trebuie verificat faptul că închiderea s-a finalizat cu succes și fără erori;
- Este interzisă efectuarea de activități neoficiale care ar putea degrada performanțele sistemelor, precum jocurile electronice;
- Participarea la jocurile de noroc sau activități ilegale care utilizează resursele IT ale organizației este strict interzisă;
- Copierea, scrierea sau execuție de cod malițios care se auto-reproduce, poate distruge sau altera informațiile, poate degrada performanțele sau încearcă să acceseze orice resursă informatică este strict interzisă;

- Este interzisă utilizarea unor facilități de tip ”Print screen” sau a unor aplicații similare) pentru a salva/imprima datele cu caracter personal afișate pe monitor;
- Scoaterea la imprimantă a datelor vehiculate (în special a datelor cu caracter personal) se va realiza numai de către utilizatori autorizați pentru această operațiune. Folosirea și distrugerea acestor materiale printate se va realiza în conformitate cu prevederile legale în vigoare cu privire la prelucrarea datelor cu caracter personal.

Stocarea datelor și arhivare

- Este interzisă utilizarea de foldere partajate la nivel local;
- Fiecare utilizator este responsabil de protecția informațiilor stocate local împotriva accesului neautorizat la respectivele resurse. De asemenea utilizatorul este responsabil de backup-ul datelor stocate local.
- Transferul de date stocate pe medii fizice trebuie să fie protejat împotriva accesului neautorizat.
- Consola sistemului trebuie blocată ori de cîte ori angajatul părăsește biroul sau nu își utilizează calculatorul;
- Angajații instituției nu vor lăsa documente pe birou la părăsirea postului de lucru;
- Angajații vor lua din imprimantă documentele proprii imediat după tipărire.

Echipamente hardware și aplicații informatice

Achiziția de echipamente hardware și de aplicații informatice

Pentru a preveni introducere de cod malițios și pentru a proteja integritatea resurselor informaționale ale instituției, toate achizițiile trebuie inițiate de responsabilul IT care administrează licențele software și echipamentele hardware, verificate de către responsabilul cu securitatea informațiilor și aprobate de către responsabilul IT.

Conformitatea cu prevederile de copyright și de licențiere; utilizarea de aplicații personale

Este permisă utilizarea exclusiv de software-ului licențiat instalat de către responsabilul IT sau firma de service.

Instalarea si/sau utilizarea de aplicații private/personale sau de aplicații care încalcă drepturile de autor pe orice sistem IT din cadrul instituției este strict interzisă.

Utilizarea mail-ului

Accesul la sistemul de mail al organizației este oferit angajaților a cător activitate de serviciu necesită utilizarea email-ului.

Scopul principal al serviciului este de a deservi realizarea activităților de serviciu în interes de organizație.

Nu este permisă utilizarea mail-ului în interes personal. Totodată, cât timp aceste mesaje rămân în sistem se consideră că sunt sub posesia și sub controlul instituției.

Utilizarea Internetului

Internetul nu asigură o conexiune sigură din perspectiva securității și nu garantează calitatea datelor.

Ca utilizator de informații, fiecare angajat este responsabil pentru a avea o atitudine profesionistă relativ la datele accesate și utilizate, mai ales la datele cu conținut dubios (email-uri sau spam, pagini de internet dubioase, cu accent în special pe inginerie socială).

Permisiuni de utilizare

Accesul remote nu este acceptat din exteriorul rețelei interne de calculatoare, iar în interior este permis doar administratorului de sistem în scopul clar de a remedia unele probleme tehnice.

Interdicții de utilizare

Violarea drepturilor de utilizare a Internetului include (fără a se limita la acestea) accesarea, descărcarea (download), trimiterea (upload), salvarea, primirea cu acceptul angajatului, sau trimiterea de materiale care includ: cconținutul sexual sau pornografic explicit; alte materiale conținând termeni vulgari, de discriminare sexuală, rasistă, de amenințare; limbaj violent sau jignitor; materiale politice/sau propagandă indiferent de motivul și scopul acestora.

Nu este permis să se utilizeze serviciile Internet pentru:

- A face publică informația confidențială proprietate a instituției fără obținerea autorizării pentru aceasta;

- Transferul materialelor a căror conținut este protejat de legea copyright-ului;
- Manipularea unor documente sau informații care, prin conținutul sau natura lor, pot aduce prejudicii materiale sau de imagine organizației sau angajaților săi, sau sunt în opoziție cu legile în vigoare;
- Transferul unir informații care încalcă normele privind protecția datelor cu caracter personal;

Este strict interzisă instalarea de gateway-uri Internet (ex. rutere WiFI), modem-uri sau a altor echipamente de rețea în cadrul rețelei interne. De asemenea nu se vor folosi conexiuni Wireless sau Bluetooth nesecurizate;

Raportare

Responsabilul IT al instituției trebuie informat imediat telefonic cu privire la orice suspiciune de manipulare neautorizată sau necorespunzătoare a datelor, furtul datelor, virusarea unui sistem IT sau alte neregularități.

Instruire

Fiecare angajat ce are acces la datele cu caracter personal din cadrul instituției trebuie să primească instructaj în vederea utilizării corespunzătoare și sigure a sistemelor de calcul. Aceștia vor fi informați cu privire la prevederile Legii nr. 679/2016 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal.

De asemenea fiecare angajat trebuie să fie conștient de politicile și de regulamentele de securitate IT disponibile pe Intranet, precum și de măsurile de contracarare și de identificare a unor posibile atacuri.

Neconformare

Toate acțiunile care contravin legilor vor fi raportate organelor competente.

Întocmit,

Persoană responsabilă cu prelucrarea datelor cu caracter personal

Didi Mariana PUIU

Tabel nominal cu salariații Muzeului Județean Botoșani
care au luat la cunoștință Regulamentul intern Securitate IT, conform Regulamentului (UE) 679/2016 al Parlamentului European privind protecția persoanelor fizice în cee ce privește prelucrarea datelor cu caracter personal

Nr. crt.	Numele și prenumele	Funcția contractuală	Semnătură
1	Alboiu Ovidiu Constantin	muzeograf	
2	Alexie Lidia	muzeograf	
3	Amarie Cristina Iuliana	muzeograf	
4	Amănălăchioaiei Simona	conservator bunuri culturale- etnografie	
5	Apăștinei Lucian Andrei	muzeograf	
6	Apopei Gheorghe	administrator	
7	Arhip George Lucian	muzeograf	
8	Caranica Emil Nicu	muzeograf	
9	Ciupu Sebastian Marcel	grafician	
10	Ciucălău Daniel	muzeograf	
11	Coșereanu Ana Elisabeta	muzeograf	
12	Epuraș Constantin	restaurator bunuri culturale-lemn	
13	Fedor Carmen Elena	referent de specialiate	
14	Hariga Daniela	referent de specialitate	
15	Iurescu Bogdana MIhaela	contabil șef	
16	Luca Marilena Daniela	referent de specialiate	
17	Kovacs Adela	muzeograf	
18	Melniciuc Aurel	manager	
	Nechifor Alexandru	consservator	
19	Penciuc Ana Alina	restaurator bunuri culturale – textile	
20	Puiu Didi Mariana	analist ajutor programator	
21	Setnic Gheorghe Eduard	șef secție	
22	Șoptelea Liviu	conservator bunuri culturale – artă	
23	Ștefură Elena Mihaela	șef secție	
24	Tocariu Maria Laura	șef secție	
25	Văculișteanu Ionuț	muzeograf	
26	Știrbăț Gheorghe Florin	muzeograf	
27	Țerna Andreea	muzeograf	