1. SCOP

Stabilește pașii ce trebuie urmați în cazul apariției unui incident de securitate care implică date cu caracter personal, pentru identificarea rapidă, notificarea autorităților și implementarea măsurilor corective.

2. DOMENIUL DE APLICARE

Se aplică tuturor facultăților, departamentelor și sistemelor informatice ale Universității Spiru Haret. Include incidente de tip pierdere, acces neautorizat, divulgare, distrugere sau alterare de date personale.

3. DOCUMENTE DE REFERINȚĂ

- Regulamentul nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (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).

4. DEFINIȚII ȘI ABREVIERI

4.1. Definiții

Incident de securitate – orice eveniment care duce la pierderea, divulgarea sau accesul neautorizat la date personale.

Notificare Data Breach – raportarea către ANSPDCP și/sau persoanele vizate.

4.2. Abrevieri

DPO – responsabilul desemnat pentru protecția datelor în cadrul universității.

5. DESCRIERE

5.1. Exemple de incidente posibile

- pierderea unui laptop sau a unui stick USB cu date personale;
- trimiterea eronată a e-mailurilor conținând date confidențiale;
- atacuri cibernetice (phishing, malware);
- acces neautorizat la sistemele informatice universitare;
- distrugerea accidentală a bazelor de date.

5.2. Etapele de gestionare a unui incident

1. Identificarea și raportarea incidentului către DPO (prin e-mail, formular sau telefonic).
2. Evaluarea de către DPO: natura incidentului, volumul datelor afectate, consecințe și riscuri.
3. Notificarea ANSPDCP în termen de 72 ore, dacă incidentul afectează drepturile persoanelor vizate.
4. Informarea persoanelor vizate, dacă este cazul, prin e-mail sau alte mijloace.
5. Documentarea completă și implementarea măsurilor corective.

5.3. Arhivarea și păstrarea documentelor

Toate incidentele sunt înregistrate într-un Registru al incidentelor de securitate, păstrat timp de minimum 5 ani. Raportul final conține descrierea, cauzele, persoanele implicate, măsurile corective și statusul remedierii.

6. RESPONSABILITĂȚI PRIVIND PROCEDURA

a. Senatul Universității
- aprobă procedura;
- aprobă reviziile procedurii.

b. Rectorul Universității
- dispune aplicarea procedurii;
- aprobă măsurile corective
- sprijină comunicarea oficială.

c. Responsabilul cu protecția datelor desemnat de universitate
- monitorizează aplicarea procedurii;
- coordonează gestionarea, documentarea și notificarea incidentelor.;
- avizează implementarea/modificarea/retragerea procedurii
- revizuiește procedura anual, ori de câte ori apar modificări legislative sau sau tehnologice;
- elaborează, verifică, difuzează, înregistrează, arhivează procedura.

d. Direcția IT
- asigură suport tehnic
- asigură implementarea măsurilor de securitate

e. Decanii, directorii de departamente, directorii școlilor doctorale, personalul didactic, secretariatele, alte categorii de angajați
- raportează imediat incidentele

7. AVIZĂRI, MODIFICĂRI ALE PROCEDURII

7.1. Procedura se avizează de CEAC și se aprobă de Senatul Universității *Spiru Haret.*
Pe baza experienței urmează să se formuleze propuneri de îmbunătățire a procedurii.

7.2. Modificările se inițiază de către DPO din cadrul Universității. Propunerea se înaintează CEAC prin DMC.

7.3. Modificările din capitolul 5 conduc la elaborarea unei noi ediții. Modificările din celelalte capitole conduc la revizia ediției curente.

7.4. Orice ediție sau revizie este avizată de CEAC și se aprobă de Senatul Universității *Spiru Haret.*

7.5. Procedura a fost aprobată de Senatul universitar în ședința din data de 30.03.2026

8. ANEXE

Anexa 1 – Formular de raportare incident de securitate.
Anexa 2 – Model notificare ANSPDCP.
Anexa 3 – Model informare persoane vizate.
Anexa 4 – Raport final de incident.

Președintele Senatului,
Prof. univ. dr. Florin Făinișî

Anexa 1

FORMULAR DE RAPORTARE INCIDENT DE SECURITATE (MODEL)

Gestionarea incidentelor de securitate (data breach)

Număr înregistrare: _____ **Data raportării:** ____ / ____ / _____ **Ora:** _____

Instrucțiuni de utilizare: Formularul se completează imediat după identificarea incidentului și se transmite fără întârziere către DPO / responsabilul desemnat, în acord cu procedura internă de gestionare a incidentelor de securitate.

A. Datele persoanei care raportează

Nume și prenume	.....
Funcția	.....
Structura / departamentul	.....
Telefon / e-mail	.....

B. Identificarea incidentului

Data și ora producerii / constatării	.....
Locul / sistemul afectat	.....
Persoana / structura care a constatat	.....

Tipul incidentului (bifați toate variantele aplicabile)

☐ Pierderea unui laptop / dispozitiv / document	☐ Trimitere eronată de e-mail / document
☐ Acces neautorizat la sistem / cont / fișier	☐ Divulgare accidentală a datelor
☐ Atac cibernetic (phishing, malware etc.)	☐ Distrugere / alterare accidentală a datelor
☐ Furt de echipamente / suporturi de stocare	☐ Alt tip de incident: .....

C. Descrierea incidentului

Descrieți clar ce s-a întâmplat, cum a fost identificat incidentul și care au fost împrejurările producerii acestuia.

D. Categorii de date cu caracter personal afectate

☐ Date de identificare (nume, prenume, CNP, serie/număr act)	☐ Date de contact (telefon, e-mail, adresă)
☐ Date academice / profesionale	☐ Date financiare / administrative
☐ Categorii speciale de date	☐ Credențiale / date de autentificare
☐ Nu se cunoaște încă	☐ Altele: .....

Persoane vizate estimate	☐ Studenți ☐ Cursanți ☐ Angajați ☐ Colaboratori ☐ Candidați ☐ Altele: .....
Număr estimativ de persoane vizate	....
Număr estimativ de înregistrări / documente afectate	....

E. Evaluarea impactului și a riscurilor

Nivel estimat al impactului asupra persoanelor vizate

☐ Scăzut	☐ Mediu	☐ Ridicat	☐ Nu poate fi estimat la acest moment

Consecințe posibile pentru persoanele vizate

Ex.: furt de identitate, discriminare, prejudiciu reputațional, acces neautorizat la conturi, pierderi financiare etc.

Observații privind riscul asupra drepturilor și libertăților persoanelor vizate

F. Măsuri imediate dispuse / deja implementate

Bifați măsurile aplicate până la momentul raportării

☐ Blocare cont / resetare parolă	☐ Izolare echipament / sistem
☐ Recuperare / ștergere mesaj transmis eronat	☐ Suspendare acces utilizator
☐ Backup / restaurare date	☐ Sesizare Direcția IT
☐ Informare superior ierarhic	☐ Altele: .....

Detalii privind măsurile aplicate

G. Notificări și escaladare

A fost informat DPO / responsabilul desemnat?	☐ Da ☐ Nu Data/Ora: .....
A fost informată Direcția IT?	☐ Da ☐ Nu Data/Ora: .....
Este necesară notificarea ANSPDCP?	☐ Da ☐ Nu ☐ În analiză
Este necesară informarea persoanelor vizate?	☐ Da ☐ Nu ☐ În analiză

H. Documente / dovezi anexate

Ex.: capturi de ecran, loguri, copii e-mail, raport IT, proces-verbal, listă persoane vizate etc.

I. Semnături și validare

Persoana care raportează	Nume/semnătură: .....
Superior ierarhic (după caz)	Nume/semnătură: .....
DPO / persoană desemnată	Nume/semnătură: .....
Data închiderii formularului	____ / ____ / _____

Notă de arhivare: Formularul și documentele aferente se păstrează la dosarul incidentului, ca parte a evidenței interne și a registrului incidentelor de securitate.

Anexa 2

NOTIFICARE ANSPDCP (MODEL)

Notificare de încălcare a securității datelor cu caracter personal

Se completează de către operatorul de date / instituția notificatoare și se utilizează pentru raportarea către ANSPDCP, în concordanță cu procedura internă privind gestionarea incidentelor de securitate și cu formularul online ANSPDCP.

Nr. intern notificare	....	**Data întocmirii**	..... / ..... / .....
Notificare	☐ inițială ☐ completare	**Nr. înregistrare ANSPDCP**	....

1. Identificarea operatorului

Denumirea operatorului / instituției	
Tip operator	
CIF/CUI	
Sediul / adresa completă	
Persoană de contact pentru notificare	
Date de contact	Telefon: ..... E-mail: .....

2. Responsabilul cu protecția datelor / punct de contact

Nume și prenume	
Funcție / calitate	
Adresă / sediu	
Date de contact	Telefon: ..... E-mail: .....

3. Informații inițiale privind incidentul

Data și ora incidentului	Data: ..... / ..... / ..... Ora: ..... : ..... ☐ estimate
Data și ora depistării	Data: ..... / ..... / ..... Ora: ..... : .....
Caracterul încălcării	☐ confidențialitate ☐ integritate ☐ disponibilitate ☐ altul: .....

Natura și conținutul datelor afectate	
Sisteme / suporturi implicate	
Alți operatori / persoane împuternicite implicate	☐ Nu ☐ Da, detalii: .....

4. Rezumatul incidentului *(includeți contextul, localizarea fizică și suporturile de stocare implicate)*

.....
.....
.....
.....
.....

5. Numărul persoanelor vizate afectate *(estimare, dacă este cazul)*

.....
.....

6. Eventualele consecințe și efecte adverse pentru persoanele vizate

.....
.....
.....
.....

7. Măsurile tehnice și organizatorice luate / propuse pentru atenuarea efectelor

.....
.....
.....
.....

8. Informarea persoanelor vizate

Persoanele vizate au fost informate?	☐ Da ☐ Nu
Număr persoane informate	
Mijloace de comunicare utilizate	☐ e-mail ☐ telefon ☐ poștă ☐ comunicare publică ☐ altul: .....

9. Conținutul informării transmise sau motivele pentru care persoanele vizate nu au fost informate

.....
.....
.....
.....
.....

10. Aspecte transfrontaliere

Sunt implicate persoane vizate din alte state membre UE?	☐ Da ☐ Nu

Au fost notificate alte autorități competente?	☐ Da ☐ Nu
Dacă da, menționați autoritățile	

11. Documente anexate

Document / dovadă anexată	**Anexat**
Raport intern al incidentului	☐ Da ☐ Nu
Capturi de ecran / log-uri / dovezi tehnice	☐ Da ☐ Nu
Informarea persoanelor vizate	☐ Da ☐ Nu
Măsuri corective dispuse	☐ Da ☐ Nu
Punct de vedere IT / DPO	☐ Da ☐ Nu

Observație: Procedura internă prevede notificarea ANSPDCP în termen de 72 de ore atunci când incidentul poate afecta drepturile persoanelor vizate.

Întocmit de	**Verificat de**	**Aprobat / transmis de**
.....	.....	.....
Nume, funcție, semnătură	Nume, funcție, semnătură	Nume, funcție, semnătură

Anexa 3

INFORMARE PERSOANE VIZATE (MODEL)

Procedura PO(S)-38 – Gestionare a incidentelor de securitate (data breach)

Model utilizat pentru comunicarea către persoanele vizate în situația în care incidentul de securitate este susceptibil să genereze un risc ridicat pentru drepturile și libertățile acestora.

Instituția / operatorul de date	.....
Nr. / data comunicării	.....
Canal de transmitere	.....
Persoana vizată	.....
Date de contact pentru răspuns	.....

1. Obiectul informării

Vă informăm că Universitatea Spiru Haret a identificat un incident de securitate care a implicat date cu caracter personal și care v-ar putea afecta în mod direct.

2. Data și împrejurările incidentului

Incidentul a fost constatat la data de ....., iar analiza internă a arătat că acesta s-a produs / ar fi putut să se producă în intervalul .....

Descriere succintă a incidentului:

.....

.....

.....

3. Categoriile de date cu caracter personal afectate

În funcție de concluziile analizei, incidentul a vizat următoarele categorii de date:

☐ date de identificare (nume, prenume, CNP, serie/număr act)

☐ date de contact (adresă, e-mail, telefon)

☐ date academice / profesionale

☐ date financiare

☐ credențiale / conturi informatice

☐ alte date: .....

4. Consecințe probabile pentru persoana vizată

Pot exista consecințe precum: acces neautorizat la informații, divulgare accidentală, utilizare frauduloasă a datelor, tentativă de phishing sau alte efecte negative asupra confidențialității datelor dumneavoastră.

Evaluarea concretă pentru cazul de față:

.....

.....

5. Măsurile luate de universitate

Universitatea a adoptat / dispus următoarele măsuri pentru limitarea efectelor incidentului și prevenirea repetării acestuia:

.....

.....

.....

6. Măsuri recomandate persoanei vizate

Vă recomandăm, după caz:

– să manifestați prudență față de mesaje, apeluri sau solicitări neobișnuite;

– să schimbați parolele / credențialele, dacă acestea ar fi putut fi compromise;

– să monitorizați conturile sau documentele relevante;

– să ne contactați imediat dacă observați utilizări neautorizate ale datelor dumneavoastră;

– alte recomandări specifice: .....

7. Date de contact DPO / punct de contact

Pentru informații suplimentare, clarificări sau exercitarea drepturilor dumneavoastră, ne puteți contacta la:

Responsabil cu protecția datelor / punct de contact: .....

E-mail: ..... Telefon: .....

8. Mențiuni finale

Regretăm incidentul produs și vă asigurăm că tratăm cu maximă seriozitate protecția datelor cu caracter personal. Situația a fost analizată conform procedurilor interne, iar măsurile necesare au fost dispuse în raport cu natura și impactul incidentului.

Funcția emitentului	**Semnătură / validare**
.....	.....

Model intern orientativ – se completează și se adaptează în funcție de natura incidentului și de categoria persoanelor vizate.

Anexa 4

RAPORT FINAL DE INCIDENT (MODEL)

Procedura PO(S)-38 - Gestionarea incidentelor de securitate (data breach)

Model utilizat pentru documentarea completă a incidentului, a analizei efectuate, a măsurilor dispuse și a statusului remedierii. Raportul final se arhivează împreună cu documentele incidentei, conform procedurii interne.

Instituția / structura raportantă	.....
Nr. raport / data întocmirii	.....
Persoana care întocmește raportul	.....
DPO / punct de contact	.....
Perioada analizată	.....
Clasificare incident	□ confidențialitate □ integritate □ disponibilitate □ mixt

1. Identificarea și descrierea incidentului

Data și modul constatării: .....
Locul / sistemul / aplicația afectată: .....
Descriere succintă a incidentului:
.....
.....
.....
.....

Categorii de persoane vizate implicate:
□ candidați / studenți
□ cursanți / doctoranzi
□ cadre didactice / personal
□ colaboratori / parteneri
□ alte persoane vizate: .....

2. Evaluarea impactului asupra datelor și persoanelor vizate

Tipuri de date afectate:
□ date de identificare
□ date de contact
□ date academice / profesionale
□ date financiare
□ credențiale / conturi informatice
□ categorii speciale de date
□ alte date: .....

Volumul estimat al datelor / numărul înregistrărilor afectate: .....
Numărul estimat al persoanelor vizate afectate: .....
Datele au fost: □ accesate neautorizat □ divulgate □ pierdute □ alterate □ indisponibile

3. Analiza cauzelor și persoane implicate

Cauza probabilă / confirmată a incidentului:
.....
.....
.....

Factori favorizanți / vulnerabilități identificate:
.....
.....
.....

Persoane / funcții / structuri implicate în analiză și intervenție:
.....
.....
.....

4. Evaluarea consecințelor și obligațiilor de notificare

Consecințe constatate sau probabile pentru persoanele vizate și pentru universitate:
.....
.....
.....
.....

Nivelul de risc stabilit: □ scăzut □ mediu □ ridicat
A fost necesară notificarea ANSPDCP? □ da □ nu
A fost necesară informarea persoanelor vizate? □ da □ nu
Observații privind termenul de 72 de ore / justificări: .....

5. Măsuri dispuse și plan de remediere

Măsuri imediate dispuse pentru limitarea efectelor:
.....
.....
.....
.....

Măsuri corective și preventive aprobate:
.....
.....
.....
.....

Responsabili de implementare și termene:
.....
.....
.....

6. Documente suport și arhivare

Documente analizate / anexate la raport:
□ formular inițial de raportare incident
□ notificare ANSPDCP
□ informare persoane vizate

□ loguri / capturi / dovezi tehnice
□ corespondență internă / externă
□ alte documente: .....
Observații privind trasabilitatea și arhivarea documentelor:
.....
.....
.....

7. Statusul remedierii și concluzii finale

Statusul implementării măsurilor la data raportului:
□ finalizat integral □ în curs □ parțial implementat □ necesită monitorizare suplimentară
Data estimată a închiderii complete a incidentului: .....
Lecții învățate / propuneri de îmbunătățire a procedurii și a controalelor interne:
.....
.....
.....
.....
Concluzie finală privind remedierea incidentului:
.....
.....
.....

8. Validare și închidere

Raportul final sintetizează analiza incidentului și măsurile dispuse, în concordanță cu procedura internă de gestionare a incidentelor de securitate. Se completează după finalizarea etapei de analiză și după stabilirea măsurilor corective și a statusului remedierii.

Întocmit de	**Avizat de**	**Aprobat / validat**
.....	.....	.....

Model intern orientativ - se completează și se adaptează în funcție de natura incidentului, concluziile analizei și măsurile dispuse.