Direcția Digitalizare și Analiză Date

PROCEDURA OPERAŢIONALĂ

privind

testarea securității sistemelor informatice ale Universității de Vest din Timișoara

COD: PO.UVT-DDAD-02

Aprobat în Şedinţa Consiliului de Administraţie al UVT din data de 16.11.2026

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

	Elemente privind responsabilii/ operaţiunea	Numele şi prenumele	Funcţia	Data	Semnătura
	1	2	3	4	5
1.1.	Elaborat	Andrei CRĂCIUN	Director Direcţia Digitalizare şi Analiză Date, Coordonator al Programului UVT de testare a securităţii informatice	9.11.2026	[redacted]
1.2.	Verificat	Prof. univ. dr. Cosmin ENACHE	Prorector responsabil DDAD	11.11.2026	
	Aviz DPO	Denisa HÎRZA	Responsabilul cu protecţia datelor (DPO)	09.11.2026	
1.4.	Aviz juridic	Cons. Jur. Anca CICIOU	Consilier juridic	10.11.2026	
1.5.	Avizat pentru conformitate cu OSGG 600/2018	Ec. dr. Daniela Haş	Şef Corp Control Intern	11.11.2026	
1.6.	Aprobat	Prof. univ. dr. Marilen Gabriel Pirtea	Rector	12.11.2026	

2. Formular de evidenţă a modificărilor

	Ediţia sau, după caz, revizia în cadrul ediţiei	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediţiei sau revizuirii ediţiei
	1	2	3	4
2.1.	Ediţia I	X	X	

3. Formular de distribuire/difuzare

	Scopul difuzării	Exemplar nr.	Facultate/Departament	Funcţia	Numele şi prenumele	Data primirii	Semnătura
	1	2	3	4	5	6	7
3.1.	aplicare	1	Direcţia Digitalizare şi Analiză Date	Director	ANDREI CRACIUN		
3.2.	aplicare	2	Coordonatorul Programului UVT de testare a securităţii	Coordonator	ANDREI CRACIUN		
3.3.	informare	3	Responsabilul cu protecţia datelor	DPO	DENISA HÎRZA		
3.4.	informare	4	Direcţia Resurse Umane	Director	BOGDAN ALDEA		
3.5.	informare	5	Facultatea de Matematică şi Informatică	Decan	COSMIN BONCHIŞ		
3.6.	evidenţă	6	Direcţia Digitalizare şi Analiză Date	Director	ANDREI CRACIUN		
3.7.	arhivare	7	Direcţia Digitalizare şi Analiză Date	Director	ANDREI CRACIUN		

4. Scopul procedurii operaţionale

Procedura stabileşte modul în care Universitatea de Vest din Timişoara îşi testează securitatea informatică prin scanări de vulnerabilităţi, teste de penetrare şi simulări de inginerie socială. Testele se fac de personal UVT şi de voluntari voluntari, pentru ca vulnerabilităţile să fie identificate şi remediate înainte de a fi exploatate.

Procedura descrie etapele unei campanii de testare: autorizarea, desfăşurarea testelor, raportarea constatărilor, remedierea şi comunicarea rezultatelor. Testele se fac numai în baza unei autorizări scrise emise conform acestei proceduri. Orice activitate de testare fără autorizare este interzisă.

5. Domeniul de aplicare a procedurii operaţionale

Procedura se aplică testării securităţii pentru:

- serviciile expuse public: site-uri, aplicaţii web, VPN, e-mail;
- reţeaua internă şi reţelele Wi-Fi ale UVT;
- aplicaţiile folosite de cadrele didactice, voluntari şi personalul administrativ;
- simulările de phishing şi alte forme de inginerie socială la distanţă.

Sistemele deţinute şi operate de UVT se testează pe baza unei autorizări interne exprese. Sistemele operate de terţi (cloud, aplicaţii găzduite de furnizori, infrastructura furnizorilor de conectivitate) se testează în limitele politicii de testare publicate de aceştia, anexată fişei de misiune.

Procedura se aplică Direcţiei Digitalizare şi Analiză Date (DTDA), coordonatorului programului şi voluntarilor voluntari care participă la procesul de testare. La aplicarea ei participă Aprobatorul, Responsabilul cu protecţia datelor (DPO), Serviciul Consultanţă şi Avizare Juridică şi Direcţia Resurse Umane (DRU), în limitele atribuţiilor de la pct. 9.

6. Documentele de referinţă (reglementări) aplicabile activităţii procedurate

6.1. Reglementări internaţionale

- Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (GDPR), în special art. 5, 6, 29, 32, 33 şi 34, 35.

6.2. Legislaţie primară

- Legea nr. 286/2009 privind Codul penal, art. 360–365 (infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice);
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679, art. 5;
- Legea nr. 78/2014 privind reglementarea activităţii de voluntariat în România.

6.3. Legislaţie secundară

- Ordinul SGG nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităţilor publice.

6.4. Alte documente, inclusiv reglementări interne ale entităţii publice

- Carta Universităţii de Vest din Timişoara;
- Regulamentul de organizare şi funcţionare al UVT;
- Codul drepturilor şi obligaţiilor studentului;
- Decizia Rectorului privind numirea coordonatorului programului şi a persoanei delegate (Aprobator);
- notele de informare privind prelucrarea datelor cu caracter personal ale angajaţilor şi voluntarilor şi regulamentul de utilizare a sistemelor IT ale UVT.

7. Definiţii şi abrevieri ale termenilor utilizaţi în procedura operaţională

7.1. Definiţii ale termenilor

Nr. crt.	Termenul	Definiţia şi/sau, dacă este cazul, actul care defineşte termenul
1.	Procedura operaţională	Procedură care descrie o activitate sau un proces ce se desfăşoară în cadrul UVT, la nivelul uneia sau mai multor structuri organizatorice din UVT, fără aplicabilitate la nivelul întregii entităţi.
2.	Ediţie a unei proceduri operaţionale	Forma iniţială sau forma modificată (după efectuarea a trei revizii, ori atunci când modificările din structura procedurii depăşesc 50% din conţinutul reviziei anterioare).
3.	Revizia în cadrul unei ediţii	Acţiunile de modificare, adăugare, eliminare a unor informaţii, date, componente ale unei ediţii a unei proceduri, modificări ce implică de regulă sub 50% din conţinutul procedurii.
4.	Program de testare a securităţii	Programul UVT de testare a securităţii informatice, desfăşurat de DDAD cu personal UVT şi voluntari voluntari, conform prezentei proceduri.
5.	Autorizare generală	Actul semnat de Aprobator prin care se autorizează derularea programului şi se împuterniceşte Directorul DDAD să semneze fişele de misiune (Anexa 1).
6.	Fişă de misiune	Autorizarea de testare pentru o campanie, semnată de Directorul DDAD, fără de care nicio testare nu este permisă (Anexa 2).
7.	Campanie de testare	Un set de teste cu perimetru, interval şi echipă stabilite într-o fişă de misiune.
8.	Perimetru	Lista exactă a sistemelor, adreselor şi aplicaţiilor care pot fi testate într-o campanie.

9.	Infrastructură de testare desemnată	Staţiile şi maşinile virtuale puse la dispoziţie de UVT, cu adrese IP cunoscute de DDAD, din care pornesc testele.
10.	Constatare	O vulnerabilitate sau o slăbiciune identificată şi raportată conform Anexei 4.
11.	Scanare de vulnerabilităţi	Identificarea automată a slăbiciunilor cunoscute ale sistemelor din perimetru.
12.	Test de penetrare	Încercarea controlată de exploatare a unei vulnerabilităţi, pentru a evalua impactul ei real.
13.	Phishing simulat	Mesaje de tip phishing trimise controlat, pentru a măsura şi a creşte vigilenţa utilizatorilor.
14.	Aprobator	Persoana delegată prin decizie de reprezentantul legal al UVT să semneze autorizarea generală a programului.
15.	Coordonator	Cadrul didactic sau specialistul IT numit prin decizie de reprezentantul legal al UVT să coordoneze programul şi voluntarii.
16.	Voluntar	Persoană cu contract de voluntariat în vigoare, încheiat în baza Legii nr. 78/2014, selectat pe baza competenţelor dovedite înainte de efectuarea testărilor prevăzute de prezenta procedură
17.	Proprietarul sistemului	Structura care foloseşte sau administrează sistemul ori aplicaţia testată.

7.2. Abrevieri ale termenilor

Nr. crt.	Abrevierea	Termenul abreviat
1.	PO	Procedura operaţională
2.	E	Elaborare
3.	V	Verificare
4.	Av.	Avizare
5.	A	Aprobare
6.	Ap.	Aplicare
7.	Ah.	Arhivare
8.	UVT	Universitatea de Vest din Timişoara
9.	ROF	Regulament de Organizare şi Funcţionare
10.	DDAD	Direcţia Digitalizare şi Analiză Date
11.	DPO	Responsabilul cu protecţia datelor cu caracter personal
12.	DRU	Direcţia Resurse Umane
13.	GDPR	Regulamentul (UE) 2016/679 privind protecţia datelor cu caracter personal
14.	ANSPDCP	Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal
15.	DNSC	Directoratul Naţional de Securitate Cibernetică

16.	CVSS	Common Vulnerability Scoring System, sistemul de evaluare a severităţii vulnerabilităţilor
17.	DoS	Denial of Service, atac de blocare a serviciului
18.	VPN	Reţea privată virtuală
19.	SCIM	Sistemul de control intern managerial

8. Descrierea procedurii operaţionale

8.1. Principii generale şi interdicţii

Testarea se face numai în baza autorizării generale a programului (Anexa 1) şi a unei fişe de misiune în vigoare (Anexa 2). Programul se desfăşoară ca analiză internă, fără anunţ prealabil către comunitatea universitară; rezultatele se comunică în formă agregată, după remediere (pct. 8.10).

Voluntarii participă la activităţile desfăşurate în acord cu prevederile prezentei proceduri în calitate de voluntari, în condiţiile Legii nr. 78/2014 privind reglementarea activităţii de voluntariat în România, UVT îndeplinind concomitent calitatea de beneficiar al testelor şi pe cea de organizaţia-gazdă a voluntarilor.

Sunt interzise, cu excepţia unei aprobări scrise:

- atacurile de blocare a serviciilor (DoS) şi testele de stres pe sisteme de producţie;
- intruziunea fizică în clădiri sau accesul fizic la echipamente;
- modificarea sau ştergerea datelor de producţie, inclusiv note, situaţii şcolare, date financiare sau de personal;
- citirea conţinutului real al e-mailurilor, documentelor sau mesajelor utilizatorilor;
- instalarea de acces persistent sau de cod care se propagă ori se dezvoltă singur;
- accesarea datelor proprii ale voluntarului sau ale persoanelor cu care acesta are o relaţie academică directă.

8.2. Documente utilizate

Documentele aferente programului, precum şi persoanele responsabile de întocmirea şi semnarea acestora, sunt:

Document	Întocmeşte	Rezoluţie	Frecvenţă şi circuit
Autorizarea generală a programului (Anexa 1)	DDAD	Aprobatorul; avizează Directorul DDAD şi DPO aviz consultativ	La lansarea programului, pentru perioada stabilită în autorizare
Fişa de misiune (Anexa 2)	Coordonatorul	Directorul DTDA; DPO – aviz consultativ pentru phishing sau date sensibile; coordonatorul	Pentru fiecare campanie; se înregistrează şi se comunică voluntarilor înainte de start

Document	Întocmeşte	Rezoluţie	Frecvenţă şi circuit
Contractul de voluntariat, cu anexele 1–3 (Anexa 3)	Coordonatorul	Reprezentantul legal al UVT sau persoana delegată şi voluntarul; avizează s Serviciul Consultanţă şi Avizare Juridică	Pentru fiecare voluntar; se înregistrează la DRU, cu notificarea DDAD, înainte de orice activitate
Raportul de vulnerabilitate (Anexa 4)	Voluntarul	Validează coordonatorul	Pentru fiecare constatare
Registrul de remediere (Anexa 5)	Coordonatorul	Actualizează Directorul DDAD	Permanent, pe durata programului, dar nu mai mult de 3 ani de la data încetării sale, conform documentelor care atestă finalizarea testelor efectuate.

8.3. Resurse necesare

Resurse materiale: infrastructura de testare desemnată (staţii şi maşini virtuale cu adrese IP cunoscute), spaţiul de stocare criptat pentru dovezi, platforma de trimitere a simulărilor de phishing, conturile de test şi VPN-ul UVT.

Resurse umane: coordonatorul programului, personalul DDAD, voluntarii, DPO, un reprezentant al Serviciului Consultanţă şi Avizare Juridică şi un reprezentant din cadrul DRU.

Resurse financiare: Activitatea de voluntariat se desfăşoară fără remuneraţie, în condiţiile legii. Cheltuielile necesare desfăşurării activităţilor pot fi suportate din bugetul Universităţii de Vest din Timişoara (UVT), numai cu aprobarea prealabilă, în scris, şi cu respectarea legislaţiei aplicabile.

În funcţie de necesităţile identificate, UVT poate contracta şi servicii specializate pentru realizarea activităţilor prevăzute de prezenta procedură, cu respectarea condiţiilor legale. Prevederile relevante ale procedurii se aplică, în mod corespunzător, şi prestatorilor de servicii contractaţi..

8.4. Lansarea programului

1. Rectorul emite decizia de numire a coordonatorului şi a persoanei delegate să semneze autorizarea generală (Aprobator).
2. Aprobatorul semnează autorizarea generală a programului (Anexa 1), după avizul Directorului DDAD şi avizul consultativ al DPO.
3. Coordonatorul selectează şi instruieşte voluntarii după semnarea de către aceştia a contractului de voluntariat şi a anexelor acestuia (Anexa 3).
4. Contractele de voluntariat se înregistrează şi se arhivează la DRU, cu notificarea DDAD, înainte de orice activitate.

5. Programul de testare porneşte ca analiză internă, fără anunţ către angajaţi şi voluntari. Pentru simulările de phishing pe angajaţi se aplică doar măsurile minime cerute de lege, fără comunicare publică (pct. 8.8).

8.5. Desfăşurarea unei campanii

1. Coordonatorul completează propunerea de campanie în fişa de misiune (Anexa 2): perimetru, tehnici, echipă, interval.
2. DDAD şi proprietarii sistemelor confirmă perimetrul şi ferestrele de testare.
3. DPO emite un aviz cosultativ privind campania dacă aceasta include phishing sau sisteme cu date sensibile (evidenţa voluntarilor, resurse umane, financiar).
4. Directorul DDAD semnează fişa de misiune, în limitele autorizării generale. Fişa se înregistrează şi se comunică voluntarilor înainte de începerea misiunii de testare.
5. Testele se desfăşoară exclusiv în intervalul de timp aprobat, prin utilizarea infrastructurii de testare desemnate, cu asigurarea înregistrării şi monitorizării activităţilor efectuate.
6. Constatările se raportează conform pct. 8.9.
7. Campania se încheie cu un raport final şi cu ştergerea datelor de test conform pct. 8.7.

8.6. Oprirea imediată

DDAD, proprietarul sistemului sau coordonatorul pot opri oricând o campanie. Voluntarul are obligaţia de a opri imediat activitatea de testare şi de a informa coordonatorul fără întârziere, dar nu mai târziu de o oră de la constatarea situaţiei, în cazul în care:

- un serviciu devine indisponibil sau se constată o funcţionare defectuoasă a acestuia;
- obţine acces la date personale peste minimul necesar dovedirii vulnerabilităţii;
- găseşte indicii că sistemul este deja compromis de terţi;
- întâlneşte conţinut aparent ilegal;
- constată că a ieşit, chiar accidental, din perimetru.

8.7. Reguli tehnice şi protecţia datelor

- Testele pornesc numai din infrastructura de testare desemnată. Laptopurile personale se folosesc doar ca terminal de acces la aceasta, în condiţiile din Anexa 2 la contractul de voluntariat (Anexa 3 la prezenta procedură).
- Testele autentificate folosesc numai conturi de test create de DDAD, niciodată contul personal al voluntarului.
- Exploatarea se opreşte imediat după dovedirea vulnerabilităţii. Accesul la date personale se dovedeşte cu minimum de înregistrări, de preferat ale conturilor de test, fără copierea datelor.
- Dovezile (capturi, jurnale) se păstrează numai în spaţiul de stocare criptat desemnat de UVT, cu datele personale mascate.

- Datele de test se şterg în termen de 90 de zile de la data închiderii campaniei. Rapoartele şi registrul, fără date personale, se păstrează timp de 3 ani.
- Prelucrarea incidentală de date personale serveşte obligaţiei UVT de a asigura securitatea prelucrării (art. 32 GDPR). Voluntarii prelucrează date numai la instrucţiunea UVT (art. 29 GDPR).
- Dacă testele arată că există date personale care au fost deja expuse unor terţi, DDAD şi DPO evaluează de îndată obligaţia de notificare a autorităţii de supraveghere în termen de 72 de ore de la momentul constatării (art. 33 GDPR).

8.8. Reguli speciale pentru simulările de phishing

Simulările care îi implică pe angajaţii UVT se vor desfăşura cu respectarea dispoziţiilor art. 5 din Legea nr. 190/2018, respectiv: existenţa unui interes legitim justificat, informarea prealabilă a angajaţilor (dacă este cazul), verificarea imposibilităţii atingerii scopului urmărit prin folosirea unor mijloace mai puţin intruzive şi stocarea datelor cel mult 30 de zile în perimetrul asigurat intern de UVT (maşinile virtuale puse la dispoziţia voluntarilor). De asemenea:

- Fiecare campanie de phishing are autorizarea DDAD, prin fişa de misiune (Anexa 2).
- Nu se va realiza o informare publică la nivelul comunităţii universitare cu privire la desfăşurarea simulărilor. Informarea prealabilă cerută de lege se face printr-o clauză generică în notele de informare privind datele personale ale angajaţilor şi voluntarilor sau în regulamentul de utilizare a sistemelor IT, fără date, ţinte sau scenarii.
- Mesajele se trimit din platforma controlată de DDAD. Voluntarii concep scenariile şi analizează numai rezultate agregate, fără să vadă identitatea persoanelor vizate.
- Paginile de destinaţie nu reţin parolele sau datele introduse. Se înregistrează doar evenimentul: mesaj deschis, link accesat, date introduse (da/nu).
- Datele nominale se păstrează cel mult 30 de zile de la data efectuării simulărilor. La expirarea acestui termen, datele vor fi fie anonimizate şi utilizate exclusiv în scopuri statistice, astfel încât identificarea persoanelor vizate să nu mai fie posibilă, fie urmează a fi şterse definitiv.
- Rezultatele obţinute în urma desfăşurării simulărilor nu se folosesc pentru evaluarea performanţelor profesionale sau academice ale persoanelor vizate ori pentru aplicarea unor măsuri de natură disciplinară sau sancţionatorie. Persoanelor care accesează linkul utilizat în cadrul simulărilor li se va afişa imediat un mesaj educativ.
- În cadrul simulărilor nu se folosesc teme legate de salarii, sănătate, încetarea raporturilor de muncă sau alte situaţii personale ale persoanelor vizate. Nu se impersonează persoane reale, instituţii publice sau branduri externe fără acordul lor.

8.9. Raportarea constatărilor şi remedierea

Constatările critice şi ridicate se raportează coordonatorului în cel mult 24 de ore de la data constatării, iar cele care nu au caracter critic sau ridicat se raportează în cel mult 5 zile lucrătoare de la datra constatării, folosind raportul de vulnerabilitate (Anexa 4). Coordonatorul validează

constatarea şi o înregistrează în registrul de remediere (Anexa 5). Termenele-ţintă de remediere sunt:

Severitate	Termen de remediere
Critică	7 zile
Ridicată	30 de zile
Medie	90 de zile
Scăzută	La următorul ciclu de mentenanţă

8.10. Confidenţialitate şi comunicarea rezultatelor

Constatările sunt informaţii confidenţiale şi aparţin UVT. Divulgarea în afara UVT se face numai cu aprobarea scrisă a Aprobatorului sau a Rectorului. Folosirea în lucrări academice este permisă după remediere, în formă anonimizată, cu aprobarea coordonatorului co-semnată de DDAD. Vulnerabilităţile din produsele terţilor se comunică furnizorului de către UVT, prin divulgare coordonată, cu sprijinul DNSC dacă este necesar.

Pentru atingerea scopului propus şi identificarea unor soluţii optime de remediere, campaniile se desfăşoară ca analiză internă, fără anunţ prealabil către comunitatea universitară. După remedierea constatărilor critice şi ridicate, UVT poate comunica angajaţilor şi voluntarilor un rezumat agregat, indicând: numărul de constatări pe severitate, stadiul remedierii şi recomandările de comportament. Rezumatul nu conţine detalii care ar permite exploatarea şi nici rezultate nominale de phishing.

Calendarul intern nu amână obligaţiile legale, care se îndeplinesc la termenele lor:

- notificarea autorităţii de supraveghere în 72 de ore, dacă testele arată că date personale au fost deja accesate sau expuse neautorizat (art. 33 GDPR);
- informarea fără întârziere a persoanelor vizate, dacă încălcarea prezintă un risc ridicat pentru ele (art. 34 GDPR);
- raportarea incidentelor către DNSC, conform dispoziţiilor legale;
- comunicarea către furnizori a vulnerabilităţilor din produsele lor.

8.11. Protecţia voluntarilor şi sancţiuni

Activitatea desfăşurată în limitele autorizării şi ale prezentei proceduri este considerată ca fiind efectuată în numele şi cu acordul expres al UVT. La solicitarea autorităţilor competente UVT va confirma în scris scopul, obiectul şi limitele autorizării acordate. În măsura permisă de dispoziţiile legale aplicabile, UVT nu va formula plângeri şi nu va solicita despăgubiri pentru efectele neintenţionate ale testelor realizate cu respectarea regulilor impuse în acest sens.

Depăşirea intenţionată a perimetrului, folosirea constatărilor în alt scop sau divulgarea lor neautorizată produc următoarele consecinţe:

- în cazul voluntarilor care au calitatea de student al UVT, încetarea de drept a contractului de voluntariat, precum şi sesizarea Comisiei de etică universitară a UVT, în vederea analizării faptelor şi dispunerii măsurilor corespunzătoare, în limitele competenţelor acesteia.

- în cazul angajaţilor UVT, sesizarea comisiei de disciplină competente, în vederea efectuării cercetării disciplinare şi, după caz, a aplicării sancţiunilor disciplinare prevăzute de legislaţia în vigoare şi de reglementările interne ale UVT, cu respectarea procedurilor legale aplicabile.

- în cazul voluntarilor neafiliaţi UVT, răspundere conform legislaţiei în vigoare şi reglementărilor interne ale UVT, cu respectarea procedurilor legale aplicabile.

Când faptele întrunesc elementele unei infracţiuni, UVT sesizează autorităţile competente conform prevederilor legale în vigoare.

8.12. Revizuirea procedurii

Procedura se poate revizui anual, dacă se apreciază necesar, sau după orice incident produs în timpul testelor, precum şi în situaţia în care intervin modificări legislative incidente în activitatea reglementată de prezenta procedură.

9. Responsabilităţi şi răspunderi în derularea activităţii

9.1. Roluri şi responsabilităţi

Rol	Cine	Responsabilităţi
Aprobator	Persoana delegată prin decizie de reprezentantul legal al UVT	Semnează autorizarea generală a programului, aprobă excepţiile privind limitele operaţionale ale misiunii, propune eventuale sancţiuni, după caz
Coordonator	Cadru didactic sau specialist IT numit prin decizie de către reprezentantul legal al UVT	Selectează şi instruieşte voluntarii, propune campaniile, supraveghează testele, validează rapoartele, ţine registrul de remediere
Direcţia Digitalizare şi Analiză Date (DTDA)	Directorul DTDA	Confirmă perimetrul, asigură infrastructura de testare şi conturile de test, informează echipele de monitorizare, semnează fişele de misiune, aprobă excepţiile, remediază constatările
DPO	Responsabilul cu protecţia datelor	Avizează procedura, emite un aviz consultativ privind campaniile de phishing şi pe cele care ating date sensibile; evaluează, pe baza constatărilor tehnice ale DTDA, implicaţiile incidentelor asupra protecţiei datelor cu caracter personal şi formulează recomandări privind notificarea acestora.
Serviciul Consultanţă şi Avizare Juridică	Consilierul juridic	Avizează procedura şi modelele documentelor suport

Rol	Cine	Responsabilităţi
DRU	Direcţia Resurse Umane	Înregistrează contractele de voluntariat şi notifică DDAD despre finalizarea acestui demers
Voluntar	Persoană care a încheiat cu UVT un contract de voluntariat în scopul descris de prezenta procedură	Efectuează teste numai în perimetrul autorizat şi respectă celelalte prevederi din contractul de voluntariat şi anexele acestuia

9.2. Matricea responsabilităţilor

Abrevierile E, V, Av., A, Ap. şi Ah. au semnificaţia de la pct. 7.2.

Nr. crt.	Activitatea	Rector / Aprobator	DTDA	Coordonator	DPO	Serviciul Consultanţă şi Avizare Juridică	DRU	Voluntar
1.	Elaborarea şi revizuirea procedurii	A	V	E	Av.	Av.	–	–
2.	Numirea coordonatorului şi a Aprobatorului	A	E	–	–	–	–	–
3.	Autorizarea generală a programului (Anexa 1)	A	E	–	Av.	–	–	–
4.	Selecţia şi instruirea voluntarilor	–	V	E	–	–	–	Ap.
5.	Încheierea şi înregistrarea contractelor de voluntariat (Anexa 3)	A	Ap.	E	–	Av.	Ah.	Ap.
6.	Emiterea fişei de misiune (Anexa 2)	–	A	E	Av.	–	–	Ap.
7.	Desfăşurarea testelor	–	V	V	–	–	–	Ap.
8.	Raportarea constatărilor (Anexa 4)	–	–	V	–	–	–	E
9.	Remedierea constatărilor (Anexa 5)	–	Ap.	V	–	–	–	–
10.	Evaluarea şi notificarea incidentelor de date	A	E	–	Av.	–	–	–
11.	Comunicarea rezultatelor către comunitate	A	E	–	–	–	–	–
12.	Arhivarea documentelor programului	–	Ah.	–	–	–	–	–

10. Anexe, inclusiv diagrama de proces

Nr. anexă	Denumirea anexei
0	1

1	Autorizare generală privind Programul UVT de testare a securităţii informatice
2	Fişă de misiune – autorizare de testare a securităţii pentru o campanie
3	Contract de voluntariat, cu Anexa 1 – Fişa de voluntariat, Anexa 2 – Fişa de protecţie a voluntarului şi Anexa 3 – Angajament de confidenţialitate, conduită etică şi protecţia datelor
4	Raport de vulnerabilitate
5	Registrul de remediere
6	Diagrama de proces

11. Cuprins

Numărul componenţei în cadrul procedurii operaţionale	Denumirea componentei din cadrul procedurii operaţionale	Pagina
	Pagina de gardă	1
1.	Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei sau, după caz, a reviziei în cadrul ediţiei procedurii operaţionale	2
2.	Formular de evidenţă a modificărilor	3
3.	Formular de distribuire/difuzare	3
4.	Scopul procedurii operaţionale	4
5.	Domeniul de aplicare a procedurii operaţionale	4
6.	Documentele de referinţă (reglementări) aplicabile activităţii procedurale	4
7.	Definiţii şi abrevieri ale termenilor utilizaţi în procedura operaţională	5
8.	Descrierea procedurii operaţionale	7
9.	Responsabilităţi şi răspunderi în derularea activităţii	11
10.	Anexe, inclusiv diagrama de proces	13
11.	Cuprins	13

Anexa nr. 1 la PO.UVT-DDAD-02

AUTORIZARE GENERALĂ[1]

privind Programul UVT de testare a securităţii informatice

Nr. UVT2026-[ ] din [ ]

Universitatea de Vest din Timişoara, prin [persoana delegată prin Decizia nr.], în temeiul Procedurii operaţionale PO.UVT-DTDA-02:

1. autorizează derularea Programului UVT de testare a securităţii informatice în perioada [*data*] – [*data*], în domeniul de aplicare stabilit la pct. 5 al procedurii;
2. împuterniceşte Directorul DTDA să semneze fişele de misiune (Anexa 2) pentru fiecare campanie, cu respectarea interdicţiilor de la pct. 8.1 al procedurii;
3. autorizează voluntarii să testeze sistemele UVT numai în baza unei fişe de misiune în vigoare, în care sunt nominalizaţi.

Activitatea desfăşurată în limitele prezentei autorizări şi ale fişelor de misiune se face cu drept, în numele şi cu acordul UVT. Autorizarea nu acoperă nicio acţiune din afara unei fişe de misiune în vigoare.

Rol	Nume	Semnătura	Data
Aprobator			
Avizat: Director DDAD			

[1] Prezentul document constituie un model standard, cu caracter orientativ, care poate fi adaptat şi particularizat în funcţie de natura, obiectul, amploarea şi specificul activităţilor efectiv desfăşurate, cu condiţia respectării limitelor de autorizare, a prevederilor prezentei proceduri şi a dispoziţiilor legale aplicabile.

Anexa nr. 2 la PO.UVT-DDAD-02

FIŞĂ DE MISIUNE[2]

autorizare de testare a securităţii pentru o campanie

Nr. UVT2026-[ ] din [ ]

Universitatea de Vest din Timişoara, prin Directorul DTDA, în baza Autorizării generale nr. [.....] din data [.....] (Anexa 1), autorizează persoanele de la punctul 5 să testeze securitatea sistemelor de la punctul 2. Testarea se face numai în intervalul şi cu tehnicile de mai jos, conform Procedurii operaţionale PO.UVT-DDAD-02

1. Date despre campanie

Câmp	Valoare
Denumirea campaniei	Ex. Noiembrie26-
Coordonator	[nume, telefon, e-mail]
Interval	De la [data, ora] până la [data, ora]
Tip	[scanare / test de penetrare / phishing simulat]
Infrastructura de testare	[staţii / maşini virtuale; adresele IP sursă]

2. Perimetru

Sistem sau aplicaţie	Adrese IP, domenii, URL-uri	Proprietar	Operat de	Ferestre permise
[ ]	[ ]	[ ]	[UVT / furnizor; acord nr.]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]

3. Excluderi

Pe lângă interdicţiile de la pct. 8.1 al procedurii, sunt excluse: [sisteme, adrese, funcţii sau intervale excluse explicit].

4. Tehnici permise

- ☐ Scanare automată de vulnerabilităţi
- ☐ Testare manuală a aplicaţiilor web
- ☐ Testare autentificată cu conturile de test: [lista]
- ☐ Testarea reţelei interne şi a reţelelor Wi-Fi

---

[2] Prezentul document constituie un model standard, cu caracter orientativ, care poate fi adaptat şi particularizat în funcţie de natura, obiectul, amploarea şi specificul activităţilor efectiv desfăşurate, cu condiţia respectării limitelor de autorizare, a prevederilor prezentei proceduri şi a dispoziţiilor legale aplicabile.

- ☐ Încercări de autentificare, limitate la [n] pe cont pe oră
- ☐ Exploatare până la dovedirea vulnerabilității, fără alte acțiuni
- ☐ Phishing simulat prin e-mail (se completează punctul 6)
- ☐ Inginerie socială prin telefon, pe scenariile anexate

5. Echipa autorizată

Nume și prenume	Contract de voluntariat nr.	Rol în campanie	Semnătură de luare la cunoștință
[ ]	[ ]	[ ]	
[ ]	[ ]	[ ]	

6. Numai pentru phishing simulat

Câmp	Valoare
Grupul vizat	[structura / categoria; număr aproximativ de persoane]
Scenarii aprobate	[anexate, nr.]
Platforma de trimitere	[administrată de DDAD]
Clauza generică de informare (nota de informare sau regulamentul IT)	[documentul, data intrării în vigoare]
Consultarea sindicatului sau a reprezentanților angajaților	[data, nr. document]
Avizul consultativ DPO	[nr., data]
Data ștergerii datelor nominale	[cel mult 30 de zile de la trimitere]

7. Contacte pentru oprire și incidente

Rol	Nume	Telefon	E-mail
Coordonator	[ ]	[ ]	[ ]
DDAD (permanență)	[ ]	[ ]	[ ]
Proprietarul sistemului	[ ]	[ ]	[ ]
DPO	[ ]	[ ]	[ ]

Oprirea se comunică telefonic/prin intermediul serviciilor de mesagerie agreate și se confirmă în scris în aceeași zi.

8. Mențiune

Activitatea desfășurată în limitele prezentei fișe de misiune și ale autorizării generale se realizează în numele și cu acordul expres al UVT. Fișa nu acoperă nicio acțiune din afara perimetrului, intervalului sau tehnicilor de mai sus. Fiecare voluntar are la el o copie a fișei pe toată durata testelor.

9. Semnături

Rol	Nume	Semnătura	Data
Director DTDA	[ ]		
	[ ]		
Coordonator	[ ]		

Anexa nr. 3 la PO.UVT-DDAD-02

CONTRACT DE VOLUNTARIAT[3]

Nr. UVT2026-[ ] din [ ]

Art. 1. Părţile

Universitatea de Vest din Timişoara, cu sediul în Timişoara, B-dul Vasile Pârvan nr. 4, cod fiscal 4250670, reprezentată de Marilen Gabriel Pirtea, în calitate de [Rector / persoană delegată prin Decizia nr.], denumită în continuare Universitatea de Vest din Timişoara sau organizaţia-gazdă,

şi

[Nume şi prenume], CNP [ ], domiciliat în [ ], act de identitate seria [ ] nr. [ ], student la [facultatea, programul, anul], e-mail [ ], telefon [ ], denumit în continuare voluntarul,

încheie prezentul contract în baza Legii nr. 78/2014 privind reglementarea activităţii de voluntariat în România.

Art. 2. Obiectul

Voluntarul desfăşoară, fără remuneraţie, activităţile de testare a securităţii informatice descrise în Anexa 1, în cadrul Programului UVT de testare a securităţii şi conform Procedurii operaţionale PO.UVT-DDAD-02 Voluntarul testează numai sistemele din fişele de misiune în care este nominalizat.

Art. 3. Durata

Contractul se încheie pe perioada [data] – [data].

Art. 4. Drepturile voluntarului

Voluntarul are dreptul:

1. la instruire iniţială şi la supravegherea coordonatorului pe toată durata activităţii;
2. la infrastructura de testare, conturile de test şi informaţiile necesare activităţii, stabilite de comun acord;
3. la confirmarea scrisă a autorizării sale, la cererea oricărei autorităţi sau a unor terţi;
4. să nu răspundă pentru efectele neintenţionate ale testelor desfăşurate cu respectarea autorizării, a procedurii şi a anexelor;
5. la certificatul de voluntariat şi la recunoaşterea activităţii ca experienţă, în condiţiile legii;

---

[3] Prezentul document constituie un model standard, cu caracter orientativ, care poate fi adaptat şi particularizat în funcţie de natura, obiectul, amploarea şi specificul activităţilor efectiv desfăşurate, cu condiţia respectării limitelor de autorizare, a prevederilor prezentei proceduri şi a dispoziţiilor legale aplicabile.

6. la rambursarea cheltuielilor aprobate în prealabil în scris de Universitatea de Vest din Timişoara.

Art. 5. Obligaţiile voluntarului

Voluntarul se obligă:

1. să îndeplinească sarcinile din Anexa 1 şi să respecte Anexele 2 şi 3 ale prezentului contract de voluntariat;
2. să testeze numai în perimetrul, intervalul şi cu tehnicile din fişa de misiune transmise;
3. să oprească testul şi să anunţe coordonatorul în situaţiile prevăzute de PO.UVT-DDAD-02;
4. să raporteze constatările exclusiv către Universitatea de Vest din Timişoara, prin canalele stabilite;
5. să participe la instruirile organizate;
6. să execute personal obligaţiile, fără să le transmită altei persoane.

Voluntarul declară pe propria răspundere că la data efectuării testelor prevăzute de **PO.UVT-DDAD-02** are cel puţin 18 ani şi că nu a fost condamnat definitiv pentru infracţiunile prevăzute la art. 360–365 din Codul penal.

Art. 6. Drepturile şi obligaţiile organizaţiei-gazdă

Universitatea de Vest din Timişoara se obligă să instruiască voluntarul, să asigure condiţiile de siguranţă din Anexa 2, să pună la dispoziţie autorizările şi resursele necesare şi să elibereze certificatul de voluntariat. Universitatea de Vest din Timişoara are dreptul să verifice activitatea, să ceară rapoarte, să constate abaterile şi să suspende imediat accesul voluntarului la infrastructura de testare.

Art. 7. Răspunderea

Voluntarul nu răspunde pentru prejudiciile produse de testele desfăşurate cu respectarea autorizării, a procedurii şi a anexelor. Voluntarul răspunde potrivit legii pentru prejudiciile produse cu intenţie sau din culpă gravă pentru pierderea, distrugerea, modificarea sau accesarea neautorizată, prin depăşirea autorizării ori încălcarea dispoziţiilor **PO.UVT-DDAD-02**.

Art. 8. Rezultatele activităţii

Rapoartele, constatările şi dovezile aparţin organizaţiei-gazdă şi sunt confidenţiale şi nu au caracter public. Instrumentele şi scripturile cu caracter general create de voluntar rămân ale acestuia, cu condiţia să nu conţină date ale UVT. Folosirea constatărilor în lucrări academice se face conform procedurii.

Art. 9. Datele personale ale voluntarului

Universitatea de Vest din Timişoara prelucrează datele voluntarului pentru încheierea şi executarea contractului şi pentru obligaţiile legale de evidenţă. Activitatea voluntarului în infrastructura de testare este jurnalizată, pentru a dovedi respectarea autorizării.

Art. 10. Încetarea contractului

Contractul încetează:

1. la expirarea duratei;
2. prin acordul părţilor;
3. prin denunţare unilaterală de către oricare dintre părţi, cu condiţia notificării prealabile, în scris, a celeilalte părţi, cu cel puţin 15 zile calendaristice înainte de data încetării contractului (Legea nr. 78/2014, art. 11–13 şi 21);
4. cu efect imediat, prin notificarea organizaţiei-gazdă, dacă voluntarul încalcă autorizarea oferită de UVT conform PO.UVT-DDAD-02 sau Anexele 2–3 ale prezentului contract;
5. după caz, la pierderea calităţii de student, dacă părţile nu convin altfel prin act adiţional.

La încetarea contractului, orice formă de acces acordată de UVT voluntarului este revocată, iar voluntarul semnează declaraţia de ştergere din Anexa 3. Obligaţiile de confidenţialitate şi ştergere rămân în vigoare şi după încetarea acestui contract.

Art. 11. Dispoziţii finale

Orice modificare a prezentului contract se realizează prin act adiţional. Litigiile se soluţionează amiabil, iar în caz contrar de instanţele competente din Timişoara. Anexele 1–3 fac parte integrantă din contract.

Contractul de voluntariat s-a încheiat în două exemplare, câte unul pentru fiecare parte, înmânat voluntarului înainte de începerea activităţii. În situaţia în care contractul de voluntariat se semnează electronic, acesta se arhivează la DRU.

Universitatea de Vest din Timişoara	Voluntar
Marilen Gabriel Pirtea, rector	[Nume şi prenume]
Semnătura:	Semnătura:
Aviz juridic: Semnătura	Data:

Anexa 1 la contractul de voluntariat – Anexa nr. 3 la PO.UVT-DDAD-02

FIŞA DE VOLUNTARIAT[4]

Câmp	Conţinut
Voluntar	[Nume şi prenume]
Rol	Tester de securitate informatică, voluntar
Coordonator	[Nume, funcţie, contact]
Locul activităţii	Sediile UVT şi la distanţă, numai prin infrastructura de testare desemnată
Competenţe necesare	Cunoştinţe de reţele, sisteme de operare şi aplicaţii web; instruirea iniţială absolvită
Competenţe dobândite	Evaluarea vulnerabilităţilor, testare de penetrare, analiza riscului, raportare tehnică, lucru după reguli de angajament

Activităţile voluntarului:

1. scanarea de vulnerabilităţi şi analiza rezultatelor, pentru a elimina rezultatele fals-pozitive;
2. testarea manuală a aplicaţiilor, reţelei interne şi reţelelor Wi-Fi din perimetrul autorizat;
3. conceperea scenariilor de phishing simulat şi analiza rezultatelor agregate, fără acces la identitatea persoanelor vizate;
4. redactarea rapoartelor de vulnerabilitate şi propunerea măsurilor de remediere;
5. verificarea remedierilor, la cererea coordonatorului;
6. participarea la instruiri şi la şedinţele de închidere a campaniilor.

Voluntarul desfăşoară aceste activităţi numai pe baza unei fişe de misiune în vigoare, în care este nominalizat.

Universitatea de Vest din Timişoara	Voluntar
Semnătura:	Semnătura:

[4] Prezentul document constituie un model standard, cu caracter orientativ, care poate fi adaptat şi particularizat în funcţie de natura, obiectul, amploarea şi specificul activităţilor efectiv desfăşurate, cu condiţia respectării limitelor de autorizare, a prevederilor prezentei proceduri şi a dispoziţiilor legale aplicabile.

Anexa 2 la contractul de voluntariat – Anexa nr. 3 la PO.UVT-DDAD-02

FIŞA DE PROTECŢIE A VOLUNTARULUI[5]

Voluntarul [Nume şi prenume] a primit instruirea de mai jos la data de [ ] şi respectă regulile acestei fişe.

A. Securitate şi sănătate în muncă

În spaţiile UVT, voluntarul respectă instrucţiunile de securitate şi sănătate în muncă şi pe cele pentru situaţii de urgenţă, prelucrate la instruirea iniţială. Orice accident sau situaţie periculoasă se anunţă imediat coordonatorului.

B. Protecţie juridică în timpul testelor

1. Voluntarul păstrează o copie, inclusiv electronică, a fişei de misiune în vigoare.
2. Voluntarul nu testează nimic din afara perimetrului, chiar dacă i se pare inofensiv, fără acord prealabil.
3. Dacă e contactat de o persoană din afara programului în legătură cu testele, voluntarul nu dă detalii şi o îndrumă către coordonator.
4. Voluntarul opreşte testul şi anunţă coordonatorul în situaţiile de oprire din procedură.

C. Echipamente

Testele pornesc numai din infrastructura de testare desemnată de UVT (staţii sau maşini virtuale cu adrese IP cunoscute). Pe aceasta, voluntarul foloseşte numai credenţialele primite personal şi acceptă jurnalizarea activităţii.

Laptopul personal se poate folosi numai ca terminal de acces la infrastructura de testare şi numai dacă:

- are un sistem de operare suportat, cu actualizările de securitate la zi;
- are discul criptat integral şi blocare automată a ecranului;
- are protecţie antimalware activă;
- foloseşte un profil de utilizator dedicat programului.

Pe laptopul personal, voluntarul nu are voie:

- să ruleze instrumente de testare direct împotriva sistemelor UVT;
- să păstreze dovezi, date, credenţiale sau rapoarte ale programului;
- să sincronizeze materialele programului în servicii cloud personale;
- să se conecteze la infrastructura de testare din reţele publice fără VPN-ul UVT.

---

[5] [5] Prezentul document constituie un model standard, cu caracter orientativ, care poate fi adaptat şi particularizat în funcţie de natura, obiectul, amploarea şi specificul activităţilor efectiv desfăşurate, cu condiţia respectării limitelor de autorizare, a prevederilor prezentei proceduri şi a dispoziţiilor legale aplicabile.

Pierderea sau furtul unui dispozitiv folosit în program se anunță coordonatorului și Direcției Digitalizare și Analiză Date în cel mult 2 ore, pentru revocarea accesului.

Coordonator	**Voluntar**
Semnătura:	Semnătura:

Anexa 3 la contractul de voluntariat – Anexa nr. 3 la PO.UVT-DDAD-02

ANGAJAMENT DE CONFIDENŢIALITATE, CONDUITĂ ETICĂ ŞI PROTECŢIA DATELOR[6]

Subsemnatul [Nume şi prenume], voluntar în Programul UVT de testare a securităţii, mă angajez:

1. **Confidenţialitate.** Păstrez confidenţiale toate informaţiile obţinute în program: vulnerabilităţi, configuraţii, credenţiale, date personale, rezultate. Obligaţia durează pe toată durata contractului şi după încetarea lui: fără limită pentru date personale şi credenţiale, iar pentru celelalte informaţii 5 ani sau până când UVT le face publice.
2. **Nedivulgare.** Nu public, nu prezint şi nu comunic constatările terţilor, inclusiv furnizorilor sau programelor de recompensare a vulnerabilităţilor, fără acordul scris al UVT.
3. **Folosire limitată.** Folosesc informaţiile numai pentru program, niciodată în folosul meu sau al altcuiva. Nu accesez datele mele sau ale colegilor şi cadrelor didactice şi nu modific nimic legat de situaţii academice.
4. **Date personale.** Prelucrez date personale numai la instrucţiunile UVT (art. 29 GDPR), în minimul necesar dovedirii unei vulnerabilităţi. Nu copiez date personale, le maschez în dovezi şi anunţ imediat coordonatorul despre orice acces accidental.
5. **Conflict de interese.** Declar coordonatorului orice legătură personală cu un sistem sau o persoană din perimetru şi mă retrag din testarea respectivă.
6. **Conduită.** Nu folosesc constatările pentru a intimida, a obţine avantaje sau a face presiuni asupra cuiva. Anunţ coordonatorul dacă aflu despre încălcarea acestor reguli.

Declar că am citit Procedura operaţională PO.UVT-DDAD-02, fişa de misiune şi prezentul angajament. Ştiu că art. 360–365 din Codul penal sancţionează accesul şi intervenţia fără drept asupra sistemelor şi datelor informatice. Înţeleg că autorizarea UVT mă acoperă numai în limitele ei. Încălcarea angajamentului duce la încetarea contractului, la sesizarea comisiei de disciplină şi, după caz, a autorităţilor, precum şi la răspundere pentru prejudicii.

Voluntar	Data
Semnătura:	

[6] [6] Prezentul document constituie un model standard, cu caracter orientativ, care poate fi adaptat şi particularizat în funcţie de natura, obiectul, amploarea şi specificul activităţilor efectiv desfăşurate, cu condiţia respectării limitelor de autorizare, a prevederilor prezentei proceduri şi a dispoziţiilor legale aplicabile.

Declarație de ștergere (la încetarea contractului)

Declar că am șters toate datele, dovezile, credențialele și materialele programului de pe dispozitivele și conturile mele și că nu am păstrat copii.

Voluntar	Data	Confirmat de coordonator
Semnătura:		Semnătura:

Anexa nr. 4 la PO.UVT-DDAD-02

RAPORT DE VULNERABILITATE[7]

câte unul pentru fiecare constatare

Câmp	Conținut
ID	[VUL-AAAA-nnn]
Data raportării	[ ]
Raportat de	[voluntar / voluntari]
Fișa de misiune	Nr. [ ] din [ ]
Sistem, URL sau adresă	[ ]
Categorie	[de exemplu, control de acces defectuos, injecție, configurare greșită]
Severitate	[Critică / Ridicată / Medie / Scăzută]; scor CVSS [ ]
Descriere	[ce este vulnerabilitatea, pe scurt]
Pași de reproducere	[pașii exacți, cu conturile de test folosite]
Impact	[ce ar putea face un atacator real]
Dovezi	[trimitere în spațiul de stocare criptat; date personale mascate]
Date personale accesate	[Nu / Da: câte înregistrări, ce tip; DPO anunțat la data]
Recomandare de remediere	[ ]
Validat de coordonator	[nume, data]

7 7 Prezentul document constituie un model standard, cu caracter orientativ, care poate fi adaptat și particularizat în funcție de natura, obiectul, amploarea și specificul activităților efectiv desfășurate, cu condiția respectării limitelor de autorizare, a prevederilor prezentei proceduri și a dispozițiilor legale aplicabile.

Anexa nr. 5 la PO.UVT-DDAD-02

REGISTRUL DE REMEDIERE

Coordonatorul ține registrul, iar DDAD actualizează starea. Termenele urmează pct. 8.9 al procedurii. Starea poate fi: nouă, validată, în remediere, remediată, verificată sau risc acceptat.

ID	Data raportării	Sistem	Constatare	Severitate	Responsabil remediere	Termen	Stare
[VUL-AAAA-001]	[]	[]	[]	[]	[]	[]	[]
[VUL-AAAA-002]	[]	[]	[]	[]	[]	[]	[]
[VUL-AAAA-003]	[]	[]	[]	[]	[]	[]	[]

Anexa nr. 6 la PO.UVT-DDAD-02

DIAGRAMA DE PROCES

