



ZARZĄDZENIE Nr 70/2025
REKTORA UNIwersytetu w SIEDLCACH

z dnia 9 lipca 2025 roku

**w sprawie postępowania w przypadku powstania zagrożeń mających wpływ na
zapewnienie bezpieczeństwa w obiektach i na terenie UwS**

Na podstawie art. 23 ust. 2 pkt 2 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2024 r. poz. 1571 ze zm.) oraz § 13 ust. 3 pkt 25 Statutu UwS zarządza się, oraz co następuje:

§ 1

W przypadku zaistnienia zagrożenia na terenie lub w obiektach UwS, w szczególności zagrożenia dla życia, zdrowia lub mienia, każda osoba, która powzięła taką informację, jest zobowiązana niezwłocznie poinformować o tym kierownika swojej jednostki organizacyjnej albo innego przełożonego, a także osobę pełniącą dyżur na portierni.

§ 2

Wszyscy pracownicy oraz studenci UwS są zobowiązani do utrzymywania porządku i zapewniania bezpieczeństwa na terenie Uczelni, a także do podejmowania działań zapobiegających powstawaniu zagrożeń, w szczególności do

- 1) znajomości zasad postępowania zawartych w instrukcji, o której mowa w § 4;
- 2) dbania o bezpieczeństwo studentów, doktorantów, słuchaczy i pracowników UwS;
- 3) uczestniczenia w organizowanych szkoleniach i treningach ewakuacyjnych;
- 4) udziału w akcjach ratowniczych.

§ 3

1. Kierownicy jednostek organizacyjnych UwS oraz pracownicy prowadzący zajęcia ze studentami, doktorantami lub słuchaczami dokonują samodzielnie oceny stopnia zagrożenia w obiektach i salach znajdujących się na terenie UwS oraz wzywają właściwe służby porządkowo-ratownicze, a także podejmują decyzje o ewentualnej ewakuacji.
2. Po godzinach pracy oraz po zakończeniu zajęć dydaktycznych, oceny stopnia zagrożenia oraz decyzje o wezwaniu właściwych służb porządkowo-ratowniczych podejmują pracownicy pełniący dyżur w portierniach, a także – w zależności od sytuacji – kierownicy, dyrektorzy lub osoby kierujące wewnętrznymi komórkami organizacyjnymi w UwS.
3. Powrót pracowników, studentów, doktorantów, słuchaczy i innych osób do ewakuowanych wcześniej budynków możliwy jest wyłącznie z chwilą poświadczenia przez wezwane służby porządkowo-ratownicze o ustaniu zagrożenia.

§ 4

Ustala się „Instrukcję postępowania w przypadku powstania zagrożeń w obiektach i na terenie UwS (dalej zwaną instrukcją), która stanowi załącznik do niniejszego zarządzenia.

§ 5

1. Kierowników jednostek organizacyjnych zobowiązuje się do niezwłocznego zapoznania pracowników, studentów, doktorantów i słuchaczy UwS z postanowieniami niniejszego zarządzenia.
2. Kierownika Działu Administracyjno-Gospodarczego oraz kierownika Osiedla Studenckiego zobowiązuje się do zapoznania pracowników portierni z instrukcją oraz umieszczenia jej w portierniach wszystkich obiektów UwS.

§ 6

Nadzór nad realizacją postanowień niniejszego zarządzenia oraz instrukcji sprawuje specjalista ds. obronnych i sytuacji kryzysowych. Do jego obowiązków w szczególności należy:

- 1) sprawowanie nadzoru nad aktualizacją procedur i instrukcji obowiązujących na szczeblu UwS, dotyczących zdarzeń określonych w załączniku do niniejszego zarządzenia;
- 2) dokonywanie losowego sprawdzenia znajomości procedur przez personel portierni;
- 3) gromadzenie informacji dotyczących okoliczności zaistniałych zdarzeń w zakresie ochrony osób i mienia oraz opracowywanie wniosków i rekomendacji mających na celu zapobieganie podobnym zdarzeniom w przyszłości;
- 4) prowadzenie szkoleń z zakresu ochrony, osób i mienia i obiektów;
- 5) współdziałanie z właściwymi służbami porządkowo-ratowniczymi.

§ 7

Traci moc zarządzenie nr 49/2014 Rektora Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach z dnia 6 czerwca 2014 roku w sprawie postępowania w przypadku powstania zagrożenia w obiektach i na terenie UPH

§ 8

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR

prof. dr hab. Mirosław Minkina

**INSTRUKCJA POSTĘPOWANIA
W PRZYPADKU WYSTĄPIENIA ZAGROŻEŃ MAJĄCYCH WPŁYW NA ZAPEWNIENIE
BEZPIECZEŃSTWA W OBIEKTACH I NA TERENIE UNIwersYTETU W SIEDLCACH**

Spis treści

I. Instrukcja postępowania w przypadku zaobserwowania wypadku na terenie Uniwersytetu	2
II. Instrukcja postępowania w przypadku próby nieautoryzowanego prowadzenia uwieczniania obiektów uczelni oraz osób znajdujących się na jej terenie	4
III. Instrukcja postępowania w przypadku próby napadu, włamania lub kradzieży.	6
IV. Instrukcja postępowania w przypadku skażeń biologicznych lub chemicznych.	8
V. Instrukcja postępowania w przypadku otrzymania telefonicznej informacji o podłożeniu ładunku wybuchowego.	10
VI. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.	12
VII. Instrukcja postępowania w związku z bezpośrednim zagrożeniem atakiem terrorystycznym związanym z zajęciem obiektu i przetrzymywaniem zakładników.	14
VIII. Instrukcja postępowania po ogłoszeniu ewakuacji.	16
IX. Instrukcja postępowania w przypadku wystąpienia zagrożenia atakiem na systemy teleinformatyczne, zwanego atakiem w cyberprzestrzeni	18

I. Instrukcja postępowania w przypadku zaobserwowania wypadku na terenie Uniwersytetu

1. Reakcja na wypadek

- W przypadku zauważenia lub odnalezienia osoby, która uległa wypadkowi, należy:
 - 1) Zachować spokój i ocenić miejsce zdarzenia pod kątem bezpieczeństwa swojego i innych osób;
 - 2) Zabezpieczyć miejsce zdarzenia – uniemożliwić dostęp osobom postronnym;
 - 3) Poinformować niezwłocznie:
 - administratora obiektu lub służbę portierską,
 - albo samodzielnie wezwać odpowiednie służby ratunkowe – tel. 112 (ogólny numer alarmowy) lub 999 (pogotowie ratunkowe).
 - 4) Poinformować osoby znajdujące się w pobliżu o potencjalnym zagrożeniu oraz poprosić o wsparcie w działaniach pomocowych.
 - 5) Sprawdzić stan poszkodowanego – przytomność, oddech, widoczne obrażenia.
 - 6) Udzielić pierwszej pomocy zgodnie z obowiązującymi zasadami.
 - 7) Zgłosić wypadek odpowiednim osobom:
 - Pracownik - przełożonemu lub do Głównemu Specjaliście ds. BHP – tel. 25 643 19 50,
 - Student - prowadzącemu zajęcia lub do dziekanatu,
 - osoba postronna/nie będąca studentem ani pracownikiem uniwersytetu - pracownikowi administracyjnemu lub służbie portierskiej.

2. Zasady udzielania pierwszej pomocy

Przede wszystkim zadbaj o swoje bezpieczeństwo abyś mógł bezpiecznie pomóc.

Dlaczego warto działać natychmiast?

- 1) Każda sekunda może decydować o życiu lub zdrowiu poszkodowanego. Wczesne rozpoczęcie działań ratunkowych zwiększa szanse przeżycia i zmniejsza ryzyko powikłań.

Czym jest pierwsza pomoc?

- 2) To natychmiastowe czynności podejmowane w razie wypadku, urazu lub nagłego zachorowania, których celem jest podtrzymanie życia lub ograniczenie skutków zdarzenia.

Kto ma obowiązek udzielić pierwszej pomocy?

- 3) Każdy. Obowiązek ten wynika z art. 162 Kodeksu karnego – nieudzielenie pomocy osobie w stanie zagrożenia życia grozi karą do 3 lat pozbawienia wolności.

3. Algorytm udzielania pierwszej pomocy

Jeśli osoba jest przytomna i oddycha:

- 1) Zapytaj, co się stało.
- 2) Oceń stan fizyczny poszkodowanego.
- 3) W razie potrzeby zabezpiecz urazy, obserwuj i uspokajaj poszkodowanego do przyjazdu służb.

Jeśli osoba jest nieprzytomna, ale oddycha:

- 1) Udrożnij drogi oddechowe (odchylenie głowy do tyłu).

- 2) Ułóż poszkodowanego w pozycji bocznej bezpiecznej.
- 3) Chroń przed wychłodzeniem lub przegrzaniem.
- 4) Obserwuj oddech do momentu przybycia zespołu ratownictwa.
- 5) Jeśli oczekiwanie przekracza 30 minut – obróć poszkodowanego na drugi bok.

Jeśli osoba nie oddycha:

Natychmiast rozpocznij resuscytację krążeniowo-oddechową (RKO):

- 1) 30 uciśnień klatki piersiowej,
- 2) 2 oddechy ratownicze,
- 3) kontynuuj cykle aż do odzyskania przytomności lub przybycia ratowników.
- 4) Użyj AED (automatycznego defibrylatora zewnętrznego), jeśli jest dostępny w pobliżu.
- 5) u dzieci poniżej 1 roku życia – stosuj tylko 2 palce i zmniejsz siłę nacisku.
4. Bezpieczeństwo własne podczas udzielania pomocy:
 - Używaj rękawiczek jednorazowych i maseczki (jeśli są dostępne).
 - Nie narażaj się na kontakt z krwią, wydzielinami ani innymi potencjalnie zakaźnymi materiałami.
5. W każdym przypadku:
 - sporządzić adnotację w Księżce dyżurów z opisem okoliczności udzielania pomocy i realizacji procedur,
6. Wykaz telefonów alarmowych:
 - 1) Telefon Alarmowy – 112;
 - 2) Pogotowie ratunkowe – 999;
 - 3) Policja (gdy wymagana interwencja służb porządkowych)- 997;
 - 4) straż pożarna (w razie zagrożenia pożarowego) – 998;
 - 5) Straż miejska - 25 794 39 86

Firma wspomagająca ochronę obiektu – 22 560-62-22 (Stacja monitorowania alarmów).

II. Instrukcja postępowania w przypadku próby nieautoryzowanego prowadzenia uwieczniania obiektów uczelni oraz osób znajdujących się na jej terenie

1. W przypadku zaobserwowania próby wykonywania zdjęć lub nagrań bez widocznej autoryzacji:
 - 1) Podejść do osoby w sposób uprzejmy, ale stanowczy i:
 - poprosić o przedstawienie tożsamości (np. legitymacja, dowód osobisty),
 - zapytać o cel i przeznaczenie wykonywanych zdjęć lub nagrań.
 - 2) Poinformować osobę, że:
 - wykonywanie zdjęć lub nagrań na terenie uczelni wymaga wcześniejszego uzyskania zgody Rektora lub innego uprawnionego organu uczelni,
 - wizerunek osób znajdujących się na terenie uczelni jest chroniony zgodnie z przepisami o ochronie danych osobowych i prawem do wizerunku,
 - rejestrowanie obiektów uczelni może podlegać ograniczeniom ze względu na bezpieczeństwo.
 - 3) W przypadku przedstawienia zgody Rektora lub innego uprawnienia (np. pisemna zgoda, identyfikator medialny, umowa):
 - poprosić o jej okazanie,
 - zanotować szczegóły zdarzenia w Księdze Dyżurów (data, godzina, miejsce, dane osoby, charakter zgody, numer identyfikatora itp.).
 - 4) Jeżeli osoba powołuje się na akredytację dziennikarską:
 - poprosić o jej okazanie,
 - niezwłocznie powiadomić Rzecznika Prasowego uczelni,
 - nie utrudniać pracy dziennikarzom, jeśli posiadają odpowiednie uprawnienia, chyba że istnieją przesłanki do interwencji (np. zakłócanie porządku, brak zgody na rejestrację w danym miejscu).
 - 5) W przypadku odmowy współpracy lub agresywnego zachowania osoby:
 - nie podejmować samodzielnej interwencji fizycznej,
 - adekwatnie do sytuacji powiadomić ochronę lub w razie konieczności, zawiadomić Policję.
 - 6) W każdym przypadku:
 - sporządzić adnotację w Księżce dyżurów z opisem sytuacji i podjętych działań, lub notatkę służbową jako oddzielny dokument do przełożonego,
 - zabezpieczyć ewentualne dowody (np. świadków, nagrania monitoringu),
 - poinformować bezpośredniego przełożonego o zaistniałym zdarzeniu.
2. Każdorazowo po wykonaniu procedur poinformować Rzecznika Prasowego UWS oraz Specjalistę ds. obronnych i sytuacji kryzysowych o zaistniałej sytuacji.
3. Wykaz telefonów alarmowych:
 - 6) Telefon Alarmowy – 112;
 - 7) Policja - 997;
 - 8) Straż miejska - 25 794 39 86
 - 9) Pogotowie Ratunkowe - 999;
 - 10) Rzecznik Prasowy - 1918
 - 11) Dział Administracyjno-Gospodarczy - 1932;
 - 12) Firma wspomagająca ochronę obiektu – 22 560-62-22 (Stacja monitorowania alarmów).

III. Instrukcja postępowania w przypadku próby napadu, włamania lub kradzieży.

1. W przypadku próby wtargnięcia (napadu, włamania) na teren obiektu:
 - wcisnąć przycisk „Antynapadowy”;
 - poinformować osoby przebywające w budynku o zagrożeniu sygnałem „NAPAD”;
 - wezwać odpowiednie służby;
 - nie podejmować samodzielnej interwencji fizycznej,
 - w miarę możliwości uniemożliwić ucieczkę sprawców przestępstwa;
 - zabezpieczyć miejsce zdarzenia i nie dopuścić do zatarcia śladów;
 - powiadomić kierownictwo obiektu;
 - zapamiętać wygląd oraz jak najwięcej szczegółów sprawcy;
 - odnotować zdarzenie w książce dyżurów.
2. W przypadku stwierdzenia lub otrzymania informacji o kradzieży należy:
 - zabezpieczyć miejsce zdarzenia i nie dopuścić do zatarcia śladów;
 - nie podejmować samodzielnej interwencji fizycznej,
 - zamknąć wyjścia z budynku w celu uniemożliwienia ucieczki sprawcy przestępstwa;
 - powiadomić kierownictwo obiektu;
 - wezwać odpowiednie służby;
 - po przybyciu policji opisać zdarzenie oraz umożliwić im sprawne przeprowadzenie akcji;
 - odnotować zdarzenie w książce dyżurów.
3. W przypadku stwierdzenia w rejonie obiektu próby zakłócania porządku lub niszczenia mienia należy:
 - wezwać odpowiednie służby;
 - przekazać informację pracownikom portierni sąsiednich budynków w kompleksach:
 - Wydział Nauk Ścisłych i Przyrodniczych, Dom Studenta nr 1, Hala sportowa, Instytut informatyki;
 - Wydział Nauk Humanistycznych, Wydział Nauk Społecznych, Wydział Sztuki, Biblioteka Główna, Archiwum, Dom Studenta nr 2, Dom Studenta nr 4, Dom Studenta nr 5;
 - Wydział Nauk Rolniczych, Wydział nauk Medycznych i Nauk o Zdrowiu, Centrum Symulacji Medycznych;
 - powiadomić kierownictwo obiektu;
 - po przybyciu policji opisać zdarzenie oraz umożliwić jej sprawne przeprowadzenie akcji;
 - sporządzić adnotację w Książce dyżurów z opisem sytuacji i podjętych działań, lub notatkę służbową jako oddzielny dokument do przełożonego.
4. Każdorazowo po wykonaniu procedur poinformować Specjalistę ds. obronnych i sytuacji kryzysowych o zaistniałej sytuacji.
5. Wykaz telefonów alarmowych:
 - 13) Telefon Alarmowy – 112;

- 14) Policja - 997;
- 15) Państwowa Straż Pożarna - 998;
- 16) Pogotowie Ratunkowe - 999;
- 17) Starszy Specjalista ds. Administracyjnych -.....; *(wpisać w wolne miejsce odpowiednio do obiektu, w którym powyższa instrukcja zostaje zaimplementowana);*
- 18) Specjalista ds. obronnych i sytuacji kryzysowych - 1120;
- 19) Dział Administracyjno-Gospodarczy - 1932;
- 20) Firma wspomagająca ochronę obiektu - 22 560-62-22 (Stacja monitorowania alarmów).

IV. Instrukcja postępowania w przypadku skażeń biologicznych lub chemicznych.

1. W przypadku otrzymania informacji o zewnętrznym skażeniu biologicznym lub chemicznym, jeżeli przebywamy w budynku należy:
 - wezwać odpowiednie służby;
 - powiadomić kierownictwo obiektu;
 - pozostać w budynku;
 - wpuścić zagrożone osoby z zewnątrz;
 - poinformować wszystkie osoby przebywające w budynku o zagrożeniu;
 - zamknąć drzwi, okna i ograniczyć napływ skażonego powietrza;
 - unikać przebywania w piwnicach i innych nisko położonych częściach budynku;
 - utrzymać łączność z kierownictwem obiektu, informując o miejscu i liczbie osób;
 - unikać korzystania z wind – używać schodów;
 - przygotować apteczkę, dokumenty oraz telefon komórkowy z ładowarką, na wypadek ewakuacji;
 - nie opuszczać budynku do czasu odwołania zagrożenia przez służby ratownicze.
2. W przypadku otrzymania informacji o zewnętrznym skażeniu biologicznym lub chemicznym, jeżeli przebywamy poza budynkiem należy:
 - schronić się w najbliższym budynku zasłaniając drogi oddechowe,
 - wezwać odpowiednie służby,
 - powiadomić kierownictwo obiektu,
 - zostawić odzież wierzchnią i buty przed wejściem - w przypadku kontaktu z niebezpiecznymi substancjami,
 - umyć dokładnie twarz i ręce,
 - unikać dotykania twarzy, zwłaszcza ust, nosa i oczu;
 - pozostać w odizolowanym miejscu do czasu przybycia służb i zastosować się do ich poleceń.
3. W przypadku rozsypania proszku lub rozlania cieczy nieznanego pochodzenia należy:
 - wezwać służby ratownicze,
 - powiadomić kierownictwo obiektu,
 - nie dopuścić osób do kontaktu z substancją,
 - nakryć substancję (np. kocem, koszem), aby zapobiec jej rozprzestrzenianiu,
 - opuścić i zamknąć pomieszczenie,
 - umyć ręce wodą i mydłem,
 - zdjąć ubranie, jeżeli miało kontakt z podejrzaną substancją i je zabezpieczyć, jeżeli jest możliwość to umyć się pod prysznicem,
 - po kontakcie z podejrzanyymi substancjami i w obrębie skażenia nie jeść, nie pić i nie palić tytoniu;
 - oznakować miejsce zdarzenia – np. taśmą, napisem „NIEBEZPIECZEŃSTWO” lub innym dostępnym sposobem;
 - nie podejmować prób neutralizacji substancji na własną rękę.
4. W przypadku gdy pomieszczenie zostanie skażone aerozolami należy:

- wezwać służby ratownicze,
 - powiadomić kierownictwo obiektu,
 - wyłączyć wentylatory i klimatyzację w całym budynku,
 - opuścić pomieszczenie zamykając okna i drzwi,
 - sporządzić listę obecnych osób i udostępnić ją policji,
 - zachować szczególną ostrożność przy otwieraniu sąsiednich pomieszczeń – mogą być również skażone;
 - w miarę możliwości poinformować inne osoby w pobliżu o konieczności opuszczenia skażonego rejonu.
5. Każdorazowo sporządzić adnotację w Księżu dyżurów z opisem sytuacji i podjętych działań, lub notatkę służbową jako oddzielny dokument do przełożonego
6. Każdorazowo po wykonaniu procedur poinformować Specjalistę ds. obronnych i sytuacji kryzysowych o zaistniałej sytuacji.
7. Wykaz telefonów alarmowych:
- 1) Numer Alarmowy - 112;
 - 2) Policja - 997;
 - 3) Państwowa Straż Pożarna - 998;
 - 4) Pogotowie Ratunkowe - 999;
 - 5) Stacja Sanitarno-Epidemiologiczna - 25 644-20-40;
 - 6) Starszy Specjalista ds. Administracyjnych -; *(wpisać w wolne miejsce odpowiednio do obiektu, w którym powyższa instrukcja zostaje zaimplementowana);*
 - 7) Dział Administracyjno-Gospodarczy - 1932;
 - 8) Główny specjalista d/s BHP - 1950
 - 9) Specjalista ds. obronnych i sytuacji kryzysowych - 1120.

V. Instrukcja postępowania w przypadku otrzymania telefonicznej informacji o podłożeniu ładunku wybuchowego.

1. Osoba odbierająca informację powinna:
 - 1) włączyć urządzenie rejestrujące rozmowy (jeżeli jest na wyposażeniu);
 - 2) nie przerywać rozmowy;
 - 3) zachować maksymalny spokój i opanowanie;
 - 4) zanotować (zapamiętać) treść wiadomości i godzinę zgłoszenia;
 - 5) zapamiętać cechy charakterystyczne głosu (damski, męski, akcent wymowy, itp.), odgłosy słyszane w tle (ruch uliczny, głosy innych osób, zakłócenia na linii, itp.);
 - 6) powiadomić głównego użytkownika obiektu;
 - 7) wezwać odpowiednie służby;
 - 8) wcisnąć przycisk „Antynapadowy”;
 - 9) zebrać informacje o podejrzanych przedmiotach i w miarę możliwości zabezpieczyć teren wokół podejrzanego przedmiotu,
 - 10) nie przekazywać informacji o zagrożeniu przez systemy nagłośnienia lub dystrybucji informacji – poinformować osoby przełożone oraz ochronę w sposób spokojny i bez wzbudzania paniki;
 - 11) ograniczyć wszelką aktywność, w tym nie używać telefonów komórkowych ani radiotelefonów w pobliżu podejrzanego przedmiotu – może to wywołać eksplozję.
2. Zawiadamiając policję, portier lub inna osoba ma za zadanie :
 - 1) podać treść rozmowy ze zgłaszającym o podłożeniu ładunku;
 - 2) wskazać miejsce i opisać przedmiot (torbę) jeśli został zlokalizowany;
 - 3) podać numer telefonu, z którego prowadzona jest rozmowa oraz swoje nazwisko i imię;
 - 4) uzyskać od policji potwierdzenie przyjęcia powyższego zawiadomienia;
 - 5) podać dokładny adres oraz ewentualne wskazówki dojazdu (np. przez którą bramę wjazdową);
 - 6) nie podejmować prób samodzielnego przeszukiwania pomieszczeń.
3. Główny Użytkownik Obiektu:
 - 1) wzywa odpowiednie służby;
 - 2) decyduje o wyznaczeniu strefy ochronnej w części zagrożenia obiektu;
 - 3) po ogłoszeniu ewakuacji kieruje nie do czasu przybycia specjalistycznych służb;
 - 4) podczas ewakuacji dąży do zachowania spokoju, aby nie dopuścić do przejawów paniki;
 - 5) po przybyciu służb:
 - a) zapoznać z sytuacją,
 - b) zapewnić dostęp do pomieszczeń i urządzeń,
 - c) udostępnić plan obiektu, wskazać wyłączniki energii i gazu;
 - d) wskazać miejsce zbiórki dla ewakuowanych oraz osobę odpowiedzialną za weryfikację obecności.
4. Ewakuowane osoby powinny:
 - 1) zabrać ze sobą rzeczy osobiste, z którymi przyszły do pracy,
 - 2) klucze do pomieszczeń należy pozostawić w drzwiach,
 - 3) nie używać telefonów komórkowych w pobliżu potencjalnego ładunku,

- 4) nie wracać po zapomniane rzeczy do budynku bez zgody odpowiednich służb.
5. Podczas ewakuacji:
 - 1) windy powinny być zablokowane;
 - 2) należy korzystać wyłącznie ze schodów ewakuacyjnych;
 - 3) należy odnotować osoby z niepełnosprawnościami i poinformować służby o ich lokalizacji.
6. Każdorazowo sporządzić adnotację w Księżu dyżurów z opisem sytuacji i podjętych działań, lub notatkę służbową jako oddzielny dokument do przełożonego
7. Każdorazowo po wykonaniu procedur poinformować Specjalistę ds. obronnych i sytuacji kryzysowych o zaistniałej sytuacji.
8. Dodatkowo w Uniwersytecie w Siedlcach obowiązuje Zarządzenie nr 20/2025 Rektora Uniwersytetu w Siedlcach z dnia 28 lutego 2025 w sprawie zasad postępowania w przypadku uzyskania informacji o podłożeniu lub zlokalizowaniu urządzenia wybuchowego w Uniwersytecie w Siedlcach.
9. Wykaz telefonów alarmowych:
 - 1) Numer Alarmowy - 112;
 - 2) Policja - 997;
 - 3) Państwowa Straż Pożarna - 998;
 - 4) Pogotowie Ratunkowe - 999;
 - 5) Starszy Specjalista ds. Administracyjnych -; *(wpisać w wolne miejsce odpowiednio do obiektu, w którym powyższa instrukcja zostaje zaimplementowana);*
 - 6) Dział Administracyjno-Gospodarczy - 1032;
 - 7) Specjalista ds. obronnych i sytuacji kryzysowych - 1120;
 - 8) Firma wspomagająca ochronę obiektu - 22 560-62-22 (Stacja monitorowania alarmów).

VI. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.

1. Symptomy informujące o zagrożeniu po otrzymaniu przesyłki:
 - 1) brak adresu nadawcy oraz oznaczeń firm pocztowych;
 - 2) nienaturalny zapach lub przebarwienia;
 - 3) obecność proszku lub innych substancji na powierzchni koperty (opakowania) lub z niej wysypujących się;
 - 4) nadmiernie oklejona taśmą;
 - 5) dostarczona przez osobę niebędącą doręczycielem i bez informacji;
 - 6) nietypowy ciężar lub dźwięki (np. tykanie, przesuwanie się zawartości);
 - 7) podejrzane napisy, groźby, ostrzeżenia na opakowaniu lub jego widoczna prowizoryczność.
2. Osoba odbierająca podejrzaną przesyłkę niewiadomego pochodzenia powinna:
 - 1) nie otwierać przesyłki;
 - 2) nie przenosić przesyłki;
 - 3) w miarę możliwości odizolować przesyłkę lub zabezpieczyć przed dostępem innych osób;
 - 4) ograniczyć ruch powietrza w pomieszczeniu, wyłączyć systemy wentylacji i klimatyzacji, zamknąć okna;
 - 5) powiadomić właściwe służby;
 - 6) powiadomić głównego użytkownika obiektu;
 - 7) zapamiętać i przekazać służbom informacje o: sposobie dostarczenia przesyłki, czasie jej zauważenia, wyglądzie oraz wszelkich podejrzanych cechach;
 - 8) spisać dane osób obecnych w pomieszczeniu lub mających kontakt z przesyłką;
 - 9) ograniczyć wszelką aktywność w rejonie przesyłki, w tym nie używać telefonów komórkowych ani radiotelefonów w bezpośrednim sąsiedztwie przesyłki – ryzyko aktywacji ładunku.
3. W przypadku kontaktu z przesyłką:
 - 1) należy dokładnie umyć ręce wodą z mydłem (unikać pocierania oczu, nosa, ust);
 - 2) jeśli substancja osiadła na odzieży – zdjąć ją i zabezpieczyć w plastikowej torbie;
 - 3) pozostać w miejscu i czekać na instrukcje służb ratowniczych – nie opuszczać budynku bez zgody.
4. Po przybyciu służb:
 - 1) niezwłocznie przekazać wszystkie informacje dotyczące przesyłki;
 - 2) udostępnić plan pomieszczenia i wskazać drogę dotarcia do miejsca jej znalezienia;
 - 3) zastosować się do zaleceń sanepidu lub PSP, jeżeli zaistnieje podejrzenie skażenia chemicznego/biologicznego.
5. Każdorazowo sporządzić adnotację w Księżce dyżurów z opisem sytuacji i podjętych działań, lub notatkę służbową jako oddzielny dokument do przełożonego
6. Każdorazowo po wykonaniu procedur poinformować Specjalistę ds. obronnych i sytuacji kryzysowych o zaistniałej sytuacji.

7. Wykaz telefonów alarmowych:

- 1) Numer Alarmowy - 112;
- 2) Policja - 997;
- 3) Państwowa Straż Pożarna - 998;
- 4) Pogotowie Ratunkowe - 999;
- 5) Dział Administracyjno-Gospodarczy - 1932;
- 6) Specjalista ds. obronnych i sytuacji kryzysowych - 1120;
- 7) Stacja Sanitarno-Epidemiologiczna - 25 644-20-40;
- 8) Starszy Specjalista ds. Administracyjnych -; *(wpisać w wolne miejsce odpowiednio do obiektu, w którym powyższa instrukcja zostaje zaimplementowana);*

VII. Instrukcja postępowania w związku z bezpośrednim zagrożeniem atakiem terrorystycznym związanym z zajęciem obiektu i przetrzymywaniem zakładników.

1. W miarę możliwości przekazać na zewnątrz informację o zdarzeniu oraz wcisnąć przycisk „Antynapadowy”.
 - jeżeli możliwe: przekazać informacje niejawnie (np. poprzez SMS lub inny dostępny sposób);
 - wskazane: powiadomienie ochrony / przełożonego, jeśli jest to możliwe bez wzbudzania podejrzeń.
2. W przypadku uniemożliwienia bezpiecznej drogi ucieczki poddać się woli napastnika, wykonując jego polecenia bez zbędnej zwłoki oraz:
 - 1) nie prowokować agresji napastników;
 - 2) nie wykonywać telefonów bez zgody napastnika;
 - 3) w żadnym przypadku nie dawać do zrozumienia, iż napastnik został rozpoznany;
 - 4) zapamiętać jak najwięcej szczegółów mogących pomóc w identyfikacji napastników (ich rysopis, ubiór, sposób poruszania się, cechy wymowy);
 - 5) nie utrudniać napastnikowi ucieczki;
 - 6) nie wdawać się w rozmowy z napastnikami, chyba że to oni je inicjują – mówić spokojnie i rzeczowo;
 - 7) w miarę możliwości obserwować, czy mają broń, urządzenia wybuchowe, ile osób znajduje się w grupie i gdzie się przemieszczają;
 - 8) w razie przetrzymywania w grupie – wspierać się wzajemnie psychicznie, unikać paniki, utrzymywać ciszę i spokój.
3. W przypadku podjęcia działań przez wyspecjalizowane służby należy niezwłocznie zająć pozycję poza bezpośrednią strefą starcia i nie poruszać się do czasu uzyskania stosownego zezwolenia ze strony osób interweniujących w akcji;
 - służby mogą użyć hałasu, granatów hukowych, silnych komunikatów – nie reagować gwałtownie;
 - trzymać ręce uniesione, nie wykonywać żadnych gestów bez polecenia funkcjonariuszy;
 - nie zadawać pytań, nie próbować kontaktować się z bliskimi, dopóki sytuacja nie zostanie zabezpieczona.
4. Każdorazowo sporządzić adnotację w Księżu dyżurów z opisem sytuacji i podjętych działań, lub notatkę służbową jako oddzielny dokument do przełożonego
5. Każdorazowo po wykonaniu procedur i zakończeniu akcji służb poinformować Specjalistę ds. obronnych i sytuacji kryzysowych o zaistniałej sytuacji.
6. Wykaz telefonów alarmowych:
 - 1) Numer Alarmowy - 112;
 - 2) Policja - 997;
 - 3) Państwowa Straż Pożarna - 998;
 - 4) Pogotowie Ratunkowe - 999;
 - 5) Specjalista ds. obronnych i sytuacji kryzysowych - 1120;

- 6) Starszy Specjalista ds. Administracyjnych -; (wpisać w wolne miejsce odpowiednio do obiektu, w którym powyższa instrukcja zostaje zaimplementowana);
- 7) Firma wspomagająca ochronę obiektu - 22 560-62-22 (Stacja monitorowania alarmów).

VIII. Instrukcja postępowania po ogłoszeniu ewakuacji.

1. Powiadomić osoby przebywające w zagrożonym rejonie donośnym głosem „EWAKUACJA”;
2. Jeżeli w obiekcie funkcjonują sprawne techniczne środki łączności należy powiadomić osoby przebywające w zagrożonym rejonie wyraźnym komunikatem „EWAKUACJA”;
3. Opuścić pomieszczenia zabierając rzeczy osobiste (klucz zostawić w drzwiach) i udać się w kierunku wskazanym przez prowadzącego ewakuację lub zgodnie z kierunkiem oznaczonym znakami ewakuacyjnymi przestrzegając następujących zasad:
 - 1) osoby, które jako pierwsze wyszły na korytarz obowiązane są odsunąć na bok, pod ścianę, przedmioty utrudniające swobodne poruszanie się;
 - 2) należy poruszać się szybko w wyznaczonym kierunku, bez podbiegania i wyprzedzania osób znajdujących się przed nami;
 - 3) należy podporządkować się poleceniom członków zespołu kierującego ewakuacją oraz zachować dyscyplinę, spokój i ciszę;
 - 4) przy ewakuacji grupami należy zachować łączność wzrokową i słuchową pomiędzy grupami;
 - 5) w przypadku silnego zadymienia dróg ewakuacyjnych należy poruszać się wzdłuż ścian, w pozycji pochylonej;
 - 6) drogi oddechowe należy zasłonić chusteczką (w miarę możliwości zmoczoną w wodzie);
 - 7) po opuszczeniu budynku należy udać się na miejsce zbiórki w celu:
 - sprawdzenia czy wszystkie osoby opuściły budynek,
 - udzielenia potrzebną pomocy lekarskiej lub innej.
4. Osoby z niepełnosprawnościami lub o ograniczonej mobilności powinny zostać objęte pomocą ze strony wyznaczonych pracowników (zgodnie z planem ewakuacyjnym budynku);
5. Nie wolno wracać do budynku bez wyraźnej zgody służb ratowniczych lub kierownika akcji;
6. Należy odnotować wszystkie osoby, które nie dotarły do punktu zbiórki – lista powinna być przekazana osobie dowodzącej akcją służb ratowniczych;
7. W razie podejrzenia, że ktoś pozostał w budynku, należy niezwłocznie poinformować służby ratownicze (nie próbować wracać samodzielnie);
8. Jeśli miejsce zbiórki znajduje się w strefie zagrożenia wtórnego (np. dym, ogień, substancje niebezpieczne), należy udać się w sposób zorganizowany w inne bezpieczne miejsce;
9. Każdorazowo sporządzić adnotację w Księżu dyżurów z opisem sytuacji i podjętych działań, lub notatkę służbową jako oddzielny dokument do przełożonego
10. Każdorazowo po wykonaniu procedur poinformować Specjalistę ds. obronnych i sytuacji kryzysowych o zaistniałej sytuacji.

IX. Instrukcja postępowania w przypadku wystąpienia zagrożenia atakiem na systemy teleinformatyczne, zwanego atakiem w cyberprzestrzeni

1. W celu stosowania dobrych praktyk w obszarze bezpieczeństwa teleinformatycznego należy:
 - 1) nie udostępniać nikomu (przesyłać, przekazywać w rozmowie telefonicznej), pod żadnym pozorem, jakichkolwiek informacji dotyczących danych dostępowych (login, hasło) do systemów teleinformatycznych wykorzystywanych w UwS;
 - 2) stosować podstawowe zasady bezpieczeństwa przy używaniu kont i haseł tzn.:
 - a) nie używać haseł słownikowych,
 - b) nie używać haseł krótkich (poniżej 8 znaków),
 - c) używać haseł zawierających zarówno cyfry, litery (małe i duże) oraz znaki specjalne,
 - d) nie używać służbowego adresu e-mail do rejestrowania się na portalach,
 - e) nie używać tych samych haseł na różnych stronach internetowych i w systemach różnych instytucji,
 - 3) zachować szczególną ostrożność przy otwieraniu otrzymanych załączników wiadomości e-mail, a w przypadku otrzymania nieoczekiwanej przesyłki pocztowej, która zawiera załączniki lub odsyła bezpośrednio do treści stron WWW zaleca się aby nie otwierać załącznika i nie korzystać bezpośrednio z przesłanych załączników;
 - 4) dokonywać częstej aktualizacji posiadanego i używanego oprogramowania antywirusowego;
 - 5) pamiętać o zagrożeniach i konsekwencjach wynikających z nieautoryzowanego rozpowszechniania informacji wrażliwych przechowywanych na nośnikach pamięci (USB, karty pamięci, dyski przenośne) np. na skutek utraty sprzętu (kradzieży, zagubienia) lub podłączenie do niezabezpieczonego systemu - istotne jest również uświadomienie użytkownikom zagrożeń związanych z infekowaniem systemów lub wykradaniem danych np. poprzez podłączenie do komputera służbowego „obcego” urządzenia (nośnika pamięci, telefonu, tabletu itp.).
2. W przypadku otrzymania informacji o prawdopodobnych niekorzystnych działaniach w cyberprzestrzeni (ataki typu odmowa usługi DOS skierowane przeciwko serwerom WWW, włamania na strony WWW, kradzież i udostępnianie informacji wrażliwych i danych osobowych, przejmowanie kont użytkowników itp.) zaleca się:
 - 1) poinformowanie użytkowników systemów informatycznych o zagrożeniach związanych z zaistniałą sytuacją;
 - 2) dokonanie aktualizacji, w miarę możliwości, użytkowanych systemów operacyjnych,
 - 3) oprogramowania wspierającego działania serwerów i usług, oprogramowania antywirusowego i zapór sieciowych, systemów obsługi i publikacji treści (systemów zarządzania treścią) w celu wyeliminowania ewentualnych błędów i luk umożliwiających naruszenie bezpieczeństwa teleinformatycznego oraz, w miarę potrzeby, instalację i konfigurację dodatkowych narzędzi zwiększających bezpieczeństwo;

- 4) separowanie w oddzielnych katalogach plików konfiguracyjnych serwera WWW, a także plików skryptowych i wykonywalnych serwera od pozostałych plików z prawami do zapisu w katalogu;
 - 5) wyłączenie niepotrzebnych usług, kont testowych oraz sprawdzenie czy uprawnione konta nie posiadają haseł domyślnych;
 - 6) monitorowanie logów i raportów serwerów WWW pod kątem wykrycia zdarzeń mających na celu nieuprawnioną modyfikację treści serwisu WWW;
 - 7) dokonanie analizy logów uruchamianych usług sieciowych;
 - 8) dokonywanie regularnych kopii bezpieczeństwa, zwłaszcza danych krytycznych.
3. W przypadku wystąpienia zagrożenia atakiem na systemy teleinformatyczne zaleca się:
- 1) wymuszenie zmiany haseł użytkowników;
 - 2) monitorowanie logów systemowych, prób logowań za pomocą protokołu SSH;
 - 3) wyłączenie kont pracowników już nie pracujących oraz kont usług, które nie są już wykorzystywane;
 - 4) w przypadku systemów domenowych – zablokowanie kont lokalnych Administratorów i używanie jedynie kont o uprawnieniach przyznawanych przez domenę.
4. W przypadku wykrycia lub podejrzenia wykrycia zdarzenia niekorzystnego, związanego z bezpieczeństwem teleinformatycznym należy powiadomić:
- a) Dział Informatyki - 1073, 1074;
 - b) Inspektor Ochrony Danych - 1020;
 - c) Specjalistę ds. bezpieczeństwa informacji i systemów teleinformatycznych – 1737.
5. Po zgłoszeniu incydentu należy:
- 1) niezwłocznie odłączyć komputer od sieci (kabel sieciowy / Wi-Fi), nie wyłączając go, jeśli nie ma takiej wyraźnej konieczności (aby nie utracić danych z pamięci RAM);
 - 2) unikać samodzielnego podejmowania działań naprawczych (np. usuwania plików, reinstalacji), co może utrudnić analizę incydentu;
 - 3) zabezpieczyć wszelkie możliwe dane mogące posłużyć do analizy incydentu, takie jak: zrzuty ekranu, godziny i treści komunikatów, kopie podejrzanych wiadomości e-mail;
 - 4) zidentyfikować inne potencjalnie zagrożone urządzenia w najbliższym otoczeniu (np. podłączone przez USB lub współdzieloną sieć);
 - 5) czekać na instrukcje od administratora IT lub Działu informatyki.
6. Dział Informatyki, po otrzymaniu zgłoszenia, podejmuje działania:
- 1) klasyfikuje incydent zgodnie z obowiązującą polityką bezpieczeństwa informacji (np. naruszenie poufności, integralności, dostępności);
 - 2) przeprowadza analizę wstępną oraz – w razie potrzeby – izoluje pozostałe potencjalnie zagrożone systemy;
 - 3) przekazuje informację do osób odpowiedzialnych za zarządzanie incydentami oraz podejmuje działania naprawcze lub ograniczające skutki ataku;
 - 4) dokumentuje incydent (czas, źródło, sposób wykrycia, zastosowane środki zaradcze);

- 5) w przypadku naruszenia ochrony danych osobowych – współpracuje z Inspektorem Ochrony Danych w celu oceny ryzyka i ewentualnego zgłoszenia naruszenia do UODO.
10. W uzupełnieniu w Uniwersytecie w Siedlcach funkcjonuje wdrożony System Zarządzania Bezpieczeństwem Informacji w którym zostały określone procedury dotyczące incydentów. W przedmiotowym zakresie nadzór sprawuje specjalista ds. bezpieczeństwa informacji i systemów teleinformatycznych.
11. Ponadto w Uniwersytecie w Siedlcach obowiązuje Zarządzenie nr 21/2025 Rektora Uniwersytetu w Siedlcach z dnia 28 lutego 2025 w sprawie wprowadzenia i realizacji procedur związanych ze stopniami alarmowymi w Uniwersytecie w Siedlcach.