



UNIwersYTET
WARSAWski



Wydział Historii
Uniwersytetu Warszawskiego

Poradnik bezpieczeństwa

dla społeczności Wydziału Historii UW



Zapisz poniżej wypisane numery telefonów w swoich kontaktach. To ważne, by w razie potrzeby, móc szybko odnaleźć właściwy numer ratunkowy.



Ogólnopolski numer alarmowy
(można tu także wysyłać SMSy)

112

Straż Uniwersytecka

22 55 22 112

Zanim cokolwiek się wydarzy, skorzystaj z informacji, które Uniwersytet Warszawski zamieszcza na stronach:

www.bezpieczenstwo.uw.edu.pl

www.odo.uw.edu.pl

Znajdziesz tam ogromną bazę informacji i porad. Znajdź czas, by się z nimi zapoznać. Przejorny – zawsze ubezpieczony.

Poradnik powstał w trosce o bezpieczeństwo społeczności Wydziału Historii UW w oparciu o materiały poaudytowe i szkoleniowe, informacje z uniwersyteckich stron www.bezpieczenstwo.uw.edu.pl; www.odo.uw.edu.pl oraz we współpracy z Biurem ds. Bezpieczeństwa UW i Inspektorem Danych Osobowych UW. Publikacja jest bezpłatna.

W poradniku, dla zachowania przejrzystości i zwięzłości tekstu, stosowana jest forma męska w znaczeniu ogólnym - odnosi się ona do wszystkich osób, niezależnie od płci.

Przygotowanie: Agata Ignatowicz-Bocian, korekta: Marzena Burczyńska

© Wydział Historii UW, 2026

Szybka ścieżka – co zrobić najpierw

1. Najważniejsza zasada: najpierw bezpieczeństwo własne. Jeśli jest ryzyko – oddal się i wezwij pomoc.
2. Powiadom Straż Uniwersytecką: (22 55) 22 112 lub zadzwoń na 112.
3. Podaj: co się stało, gdzie (budynek/piętro/sala), ile osób poszkodowanych, swoje dane kontaktowe.
4. Ostrzegaj innych, słuchaj i wykonuj polecenia służb.
5. W razie ewakuacji – idź drogami ewakuacyjnymi do punktu zbiórki, nie używaj windy.
6. Nie nagrywaj i nie publikuj informacji o działaniach służb podczas zdarzeń kryzysowych. To może zwiększyć ryzyko.

Przycisk bezpieczeństwa

Telefony w pokojach pracy administracji mają zaprogramowany przycisk alarmowy. Po jego naciśnięciu Straż Uniwersytecka słyszy, co dzieje się w danym pomieszczeniu i może szybko zareagować w sytuacji zagrożenia. Nie trzeba wykonywać połączenia – wystarczy nacisnąć zaznaczony na zdjęciu obok przycisk.



Hasło bezpieczeństwa

Wydział posiada wewnętrzne hasło bezpieczeństwa. Informacja o hasle może być przekazana tylko pracownikom Wydziału za pośrednictwem dyrektora administracji. Po usłyszeniu hasła – telefonicznie lub osobiście – traktuj sytuację jako realną i w razie potrzeby pomóż na miejscu lub wezwij pomoc Straży Uniwersyteckiej lub 112.

Rozmieszczenie apteczek i dozowników plastrów

Chodząc po Wydziale zwróć uwagę na rozmieszczenie apteczek i dozowników plastrów. Zanim coś się wydarzy, dobrze jest wiedzieć, gdzie je najszybciej znajdziesz.

Apteczki

- **parter**
 - o na portierni
 - o przy defibrylatorze – **wolny dostęp**
- **piętro 2.**
 - o w Lektorium, za biurkiem obsługi sali
 - o na zapleczu biblioteki, przy drzwiach wejściowych
 - o w Sekcji badań i finansów (obok Sali A) na ścianie po prawej stronie drzwi wejściowych
 - o przy sali 124 – **wolny dostęp**
- **piętro 3.**
 - o w pokoju nr 1, po lewej stronie drzwi na ścianie przy zlewie
 - o w sekcji studenckiej – pok. nr 7 – na szafce przy drzwiach wejściowych
- **piętro 4**
 - o naprzeciwko windy – **wolny dostęp**

Dozowniki plastrów

- **parter**
 - o przy defibrylatorze – **wolny dostęp**
- **piętro 2.**
 - o przy wejściu do Common Roomu
 - o przy sali 124 – **wolny dostęp**
- **piętro 3**
 - o przy sekcji studenckiej (pok. nr 7) – **wolny dostęp**

Ewakuacja



Chodząc po korytarzach budynku zapoznaj się z planem dróg ewakuacyjnych (zielone porozklejane w budynku tabliczki, w którą stronę należy uciekać);



sprawdź lokalizację punktów zbiórki do ewakuacji na terenie kampusu centralnego (najbliższy na skwerze przed naszym Wydziałem). Stosuj się do poleceń służb i osób kierujących ewakuacją.

Tylko wtedy, jeżeli nie zagraża to Twojemu bezpieczeństwu:

- zakończ pracę na komputerze i zabezpiecz dane
- wyłącz i zabezpiecz urządzenia elektryczne
- zabierz rzeczy osobiste i idź do punktu zbiórki na zewnątrz

Zasady bezpiecznej ewakuacji

Podczas ewakuacji:

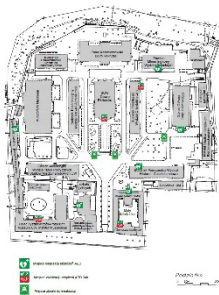
- nie zamykaj pomieszczeń na klucz
- kieruj się do najbliższego wyjścia ewakuacyjnego oznakowanymi drogami ewakuacyjnymi
- nie korzystaj z wind
- zachowaj spokój i nie wpadaj w panikę
- w miarę możliwości pomagaj osobom potrzebującym pomocy, jeśli nie zagraża to Twojemu bezpieczeństwu

W przypadku silnego zadymienia:

- poruszaj się w pozycji pochylonej
- trzymaj głowę jak najniżej poziomu podłogi
- jeśli to możliwe, zabezpiecz drogi oddechowe wilgotną chustką lub tkaniną

Po opuszczeniu budynku:

- udaj się do wyznaczonego punktu zbiórki;
- nie wracaj do budynku do czasu otrzymania zgody służb ratunkowych;
- zgłoś przełożonemu lub osobie kierującej ewakuacją informację o osobach, które mogły pozostać w budynku.



Mapa kampusu centralnego z oznaczeniami punktów zbiórki do ewakuacji oraz lokalizacji AED (w tym AED 24h) znajduje się na stronie 26.

SYTUACJE = PROCEDURY

POŻAR

Pamiętaj: Twoje bezpieczeństwo jest najważniejsze. Nigdy nie podejmuj działań gaśniczych ani ratowniczych, jeśli może to zagrażać Twojemu życiu lub zdrowiu.

W przypadku stwierdzenia pożaru:

- **powiadom służby ratunkowe – nr 112 lub Straż Uniwersytecką: tel. 22 55 22 112**
- zaalarmuj wszystkie osoby znajdujące się w strefie zagrożenia przy użyciu dostępnych środków (głośne wołanie „POŻAR”, szybki telefon, włącz przycisk bezpieczeństwa w telefonie)
- opuść budynek

Jeżeli nie zagraża to Twojemu bezpieczeństwu, pożar jest niewielki i nie stanowi bezpośredniego zagrożenia dla życia lub zdrowia, podejmij próbę jego ugaszenia przy użyciu dostępnego sprzętu gaśniczego.

BOMBA, PODEJRZANY PRZEDMIOT, NIEZNANA PRZESYŁKA

Jeżeli widzisz podejrzany przedmiot, podejrzaną przesyłkę lub otrzymałeś informację o tym, że w budynku może znajdować się bomba (mailowo, telefonicznie lub osobiście):

- **powiadom nr 112 lub Straż Uniwersytecką: tel. 22 55 22 112**
podając jak najwięcej szczegółów:
 - o skąd masz informację
 - o o jaki rodzaj zagrożenia chodzi
 - o w przypadku osobistej rozmowy postaraj się podać jej dokładną treść, jeśli to możliwe zapisz numer telefonu, z którego dzwoniono, podaj adres e-mail, z którego przekazano informację o zagrożeniu
- wyłącz wentylację i klimatyzację, zamknij okna
- nie naruszaj zawartości – nie dotykaj, nie wężaj, nie przenoś, zachowaj bezpieczną odległość
- nie używaj elektroniki w pobliżu podejrzanego obiektu
- jeśli to bezpieczne zabezpiecz przesyłkę w podwójnym worku i zaklej;
- dokładnie umyj ręce i czekaj na służby
- jeśli nie zagraża to Twojemu bezpieczeństwu do czasu przybycia służb zabezpiecz zagrożone miejsce, aby nikt się nie zbliżał, ostrzegaj innych o zagrożeniu
- po przybyciu służb wykonuj polecenia funkcjonariuszy; po ogłoszeniu ewakuacji skieruj się w miejsce wskazane przez służby (UWAGA! niekoniecznie będzie to punkt ewakuacji na terenie kampusu UW – koniecznie słuchaj poleceń służb!)
-

PIERWSZA POMOC, ZAGROŻENIE ZDROWIA LUB ŻYCIA

W razie zdarzenia, kiedy widzisz, że ktoś potrzebuje pomocy medycznej, natychmiast **powiadom służby ratunkowe – nr 112 lub Straż Uniwersytecką: tel. 22 55 22 112.**

Następnie:

- oceń bezpieczeństwo miejsca zdarzenia. Jeśli miejsce jest niebezpieczne i zagraża twojemu bezpieczeństwu – nie podchodź
- jeżeli widzisz, że nic ci nie zagraża – nie zwlekaj z udzieleniem pierwszej pomocy
- oceń stan poszkodowanego:
 - o sprawdź przytomność, delikatnie potrząsając za ramiona i pytając, czy wszystko w porządku
 - o jeśli poszkodowany jest przytomny – pozostaw go w bezpiecznej pozycji, zapytaj co się stało i obserwuj jego stan do czasu przyjazdu służb
 - o jeśli poszkodowany jest nieprzytomny – sprawdź oddech
 - o jeśli oddycha prawidłowo, ułóż go w pozycji bezpiecznej i oczekuj na wezwaną pomoc
 - o jeśli nie oddycha rozpocznij resuscytację krążeniowo-oddechową
 - o wykonuj uciski klatki piersiowej na środku mostka: 100–120 uciśnień na minutę. Jeśli potrafisz i chcesz, po 30 uciśnięciach wykonaj 2 oddechy ratownicze, jeśli nie – wykonuj same uciski
- przy portierni Wydziału, na parterze (naprzeciwko Sali Kolumnowej) znajduje się **defibrylator AED**. Nie bój się go użyć w razie potrzeby: urządzenie po otwarciu wydaje polecenia co i jak należy robić – dasz radę!
- resuscytację prowadź do momentu przyjazdu służb, odzyskania oznak życia przez poszkodowanego lub utraty własnych sił

TERRORYSTA – ZASADA 4U

UWAŻAJ

- zwracaj uwagę na nietypowe zdarzenia i zmiany w otoczeniu
- reaguj na nienaturalne i niepokojące zachowania osób

UCIEKAJ

- zostaw rzeczy – nie trać czasu
- pomagaj innym tylko jeśli to nie spowalnia ucieczki
- gdy jesteś bezpieczny – dzwoń na 112 i powiadom Straż Uniwersytecką

UKRYJ SIĘ

- schowaj się poza zasięgiem wzroku napastnika
- zamknij i zablokuj drzwi, wyłącz światła
- wycisz telefon (także wibracje) i bądź cicho
- połóż się na podłodze z dala od drzwi i okien

UDAREMNIJ ATAK

- walcz tylko, gdy nie ma innego wyjścia i zależy od tego Twoje życie
- działaj zdecydowanie, wykorzystaj zaskoczenie, współpracuj z innymi

Podczas działań służb

- połóż się, trzymaj ręce na głowie i wykonuj polecenia
- nie uciekaj bez wyraźnego rozkazu wyjścia
- nie nagrywaj i nie publikuj informacji o działaniach służb

AGRESYWNA OSOBA

W sytuacji kontaktu z osobą agresywną stosuj następujące zasady:

- unikaj bezpośredniej konfrontacji
- zachowuj bezpieczny dystans i pozostaw sobie możliwość szybkiego wyjścia z pomieszczenia
- staraj się deeskalować emocje spokojnym, rzeczowym językiem
- mów krótko i jasno, unikaj poleceń, ocen i podnoszenia głosu
- nie odpowiadaj agresją na agresję
- nie wykonuj gwałtownych ruchów i nie prowokuj gestami
- jeżeli to możliwe, wezwij wsparcie innych pracowników lub studentów (np. użyj hasła bezpieczeństwa, dyskretnie poproś osoby, które są w pobliżu o pomoc lub wezwanie Straży Uniwersyteckiej, włącz przycisk bezpieczeństwa na telefonie)
- w razie eskalacji spróbuj oddalić się w bezpieczne miejsce, wyjść z zamkniętego pomieszczenia, z budynku

To ważne, aby:

- zachować spokój i kontrolować własne emocje
- unikać stania w miejscu, z którego nie ma drogi wyjścia (np. zamknięte pomieszczenie)
- po zdarzeniu poinformować dyrektora administracji i sporządzić notatkę dotyczącą przebiegu sytuacji (dyrektor.administracji.wh@uw.edu.pl)

SKAŻENIE BIOLOGICZNE LUB CHEMICZNE

Powiadom służby ratunkowe: 112 lub Straż Uniwersytecką: tel. 22 55 22 112.

Jeśli jesteś w budynku

- pozostań w budynku i poinformuj innych
- zamknij drzwi i okna
- wyłącz klimatyzację i wentylację
- przejdź do pomieszczeń gdzie są małe okna (III piętro, sale wykładowe)
- unikaj piwnic i nisko położonych części budynku
- osłoń nos i usta wilgotną tkaniną
- czekaj na polecenia służb

Jeśli jesteś na otwartym terenie

- wejdź do najbliższego otwartego budynku
- poruszaj się prostopadle do kierunku wiatru (żeby wiatr nie wiał ci w oczy)
- po schronieniu umyj twarz, włosy i ręce, oczyść oczy i uszy
- odzież i obuwie po kontakcie z substancją zostaw przed budynkiem
- jeśli doszło do kontaktu z substancją nie dotykaj i nie wężaj jej, nie sprzątaj proszku i nie ścieraj cieczy
- przykryj substancję (np. kocem), aby ograniczyć rozprzestrzenianie
- nie jedz, nie pij i nie pal po kontakcie z podejrzaną substancją
- stosuj się do poleceń służb ratunkowych

KRYZYS ZDROWIA PSYCHICZNEGO

Jeśli widzisz u siebie lub u innej osoby objawy zagrożenia (silne pobudzenie, utrata logicznego myślenia, ryzyko zrobienia krzywdy sobie lub innym) **natychmiast wezwij pomoc: 112 lub Straż Uniwersytecką: tel. 22 55 22 112.**

Kiedy samemu skorzystać z pomocy?

Skontaktuj się z Centrum Pomocy Psychologicznej UW:

- gdy sytuacja przerasta Twoje możliwości radzenia sobie
- gdy pojawia się lęk, utrata koncentracji, rozdrażnienie, agresja, bezsenność, poczucie bezsensu
- gdy masz myśli samobójcze lub rezygnacyjne albo doświadczyłeś/aś sytuacji traumatycznej

STUDENCI

Punkt Zgłoszeniowy (bez umawiania)

poniedziałki–czwartki, godz. 10.00–14.00

Kampus Ochota, ul. Ludwika Pasteura 7, I piętro, pok. 108

Weź dowód osobisty lub legitymację studencką (wymagany aktywny status studenta)

Centrum Pomocy Psychologicznej przyjmuje także w języku:

- angielskim: wtorki 14.00–16.00, środy 10.00–14.00
- ukraińskim: wtorki 14.00–16.00

DOKTORANCI I PRACOWNICY

Umów się na spotkanie mailowo: cpp@adm.uw.edu.pl

UCZESTNICTWO W PUBLICZNYCH WYDARZENIACH NA TERENIE UW

Zanim wydarzenie się zacznie

- zwróć uwagę, gdzie znajdują się najbliższe wyjścia ewakuacyjne
- miej przy sobie naładowany telefon
- zapoznaj się z komunikatami organizatora, jeśli takie są

Tłok i nadmierne zagęszczenie

Co może się wydarzyć: ścisk, utrudnione poruszanie się, ryzyko potknięć

Jak reagować:

- zachowaj spokój i nie przepychaj się
- kieruj się do mniej zatłoczonych miejsc (wybieraj przejście bokiem, tłum w panice napiera zazwyczaj na środek)
- słuchaj poleceń organizatorów i ochrony

Alarm pożarowy lub ewakuacja

Co może się wydarzyć: sygnał alarmowy, komunikat o opuszczeniu budynku

Jak reagować:

- natychmiast przerwij udział w wydarzeniu
- kieruj się do najbliższego wyjścia ewakuacyjnego
- nie korzystaj z wind
- nie wracaj po pozostawione rzeczy
- po wyjściu udaj się do wskazanego miejsca zbiórki

Nagle pogorszenie stanu zdrowia

Co może się wydarzyć: omdlenie, uraz, atak paniki (Twój lub innej osoby)

Jak reagować:

- wezwij Straż Uniwersytecką lub zadzwoń na 112
- jeśli potrafisz, udziel pierwszej pomocy
- zapewnij poszkodowanemu przestrzeń i dopływ powietrza

Zachowania agresywne lub konflikt

Co może się wydarzyć: kłótnia, agresywne zachowanie uczestnika

Jak reagować:

- nie wdawaj się w spór
- oddal się w bezpieczne miejsce
- powiadom organizatora, Straż Uniwersytecką lub 112

Podejrzany pakunek lub niepokojąca sytuacja

Co może się wydarzyć: pozostawiona bez opieki torba, dziwne zachowanie osoby

Jak reagować:

- nie dotykaj podejrzanych przedmiotów;
- poinformuj Straż Uniwersytecką i organizatora wydarzenia;
- stosuj się do wydawanych poleceń.

Nagle załamanie pogody

Co może się wydarzyć: burza z piorunami, silny wiatr, ulewa

Jak reagować:

- słuchaj komunikatów organizatora
- udaj się do wskazanego miejsca schronienia
- unikaj drzew, masztów i metalowych konstrukcji

Awaria techniczna (np. brak prądu)

Co może się wydarzyć: zgaśnięcie światła, przerwa w wydarzeniu

Jak reagować:

- zachowaj spokój, nie panikuj
- pozostań na miejscu lub postępuj zgodnie z komunikatami
- w razie ewakuacji kieruj się oznaczeniami

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

Phishing (wyludzanie danych przez fałszywe wiadomości)

Na czym polega: podszywanie się pod zaufane instytucje w celu wyludzenia danych logowania, danych osobowych lub pieniędzy

Sygnały ostrzegawcze:

- presja czasu („pilne”, „ostatnia szansa”)
- prośba o kliknięcie w link lub podanie danych
- adres nadawcy podobny do prawdziwego
- komunikaty wzbudzające strach

Jak postępować:

- nie klikaj w linki ani załączniki
- zweryfikuj wiadomość innym kanałem
- zgłoś do IT UW mailowo lub telefonicznie: abuse@uw.edu.pl; 22 55 20 527 (zgłoszeń można dokonywać przez całą dobę)

Malware (złośliwe oprogramowanie)

Na czym polega: program instalowany bez wiedzy użytkownika w celu kradzieży danych, szpiegowania lub przejęcia kontroli nad urządzeniem

Najczęstsze drogi infekcji:

- podejrzanе załączniki
- niebezpieczne linki
- nieautoryzowane programy
- zainfekowane pendrive'y

Jak postępować:

- aktualizuj system i aplikacje
- używaj programu antywirusowego
- instaluj oprogramowanie tylko z zaufanych źródeł

Ransomware (oprogramowanie blokujące dane dla okupu)

Na czym polega: złośliwy program szyfruje pliki i żąda zapłaty za ich odblokowanie

Skutki:

- utrata dostępu do dokumentów
- paraliż pracy
- ryzyko trwałej utraty danych

Jak postępować:

- wykonuj regularne kopie zapasowe
- aktualizuj oprogramowanie
- nie otwieraj podejrzanych plików
- nie płać okupu

Smishing (wyludzanie danych przez fałszywe SMS-y)

Na czym polega: oszustwo polegające na wysyłaniu SMS-ów z linkiem do fałszywej strony

Typowe przynęty:

- dopłata do przesyłki
- blokada konta
- informacja o nagrodzie

Jak postępować:

- nie klikaj w linki z SMS
- sprawdzaj sprawę na oficjalnej stronie
- zachowaj ostrożność wobec „pilnych” wiadomości

Vishing (wyludzanie danych przez telefon)

Na czym polega: oszust dzwoni, podszywając się np. pod bank, dział IT lub przełożonego

Czego mogą chcieć:

- hasła
- kody autoryzacyjne
- wykonania przelewu
- instalacji programu

Jak postępować:

- nigdy nie podawaj haseł przez telefon
- zakończ rozmowę
- oddzwoń na oficjalny numer

Kluczowe zasady cyberhigieny

- regularnie instaluj poprawki systemu, aplikacji i antywirusa
- stosuj silne hasła oraz 2FA, czyli uwierzytelnianie dwuetapowe (Two-Factor Authentication)

Czym jest 2 FA?

To zabezpieczenie, dzięki któremu poznanie Twojego hasła nie wystarczy, aby ktoś włamał się na Twoje konto.

Polega ono na tym, że oprócz hasła musisz podać drugi element potwierdzający tożsamość, np.: kod SMS, kod ze specjalnej aplikacji (np. Google Authenticator lub Microsoft Authenticator), powiadomienie push w telefonie lub musisz użyć tokena.

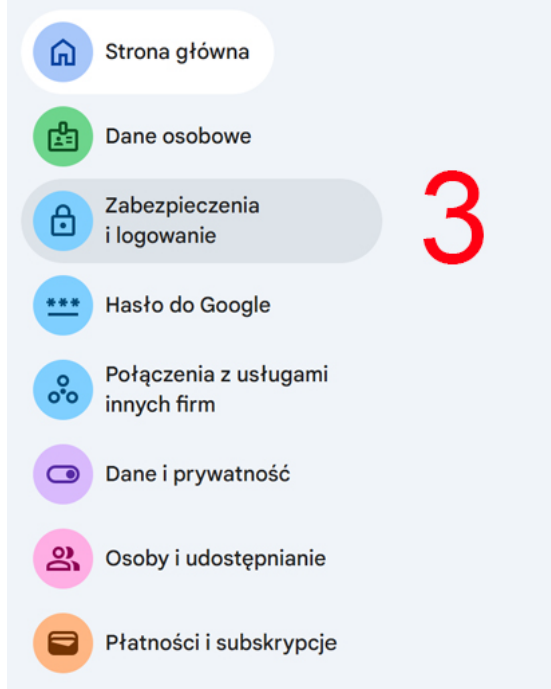
Jak włączyć uwierzytelnianie 2FA?



1. Zaloguj się do swojego e-maila.

2. Wejdź w „Zarządzaj kontem Google”

Google Konto



3. Następnie wybierz „Zabezpieczenia i logowanie” i tam włącz „Uwierzytelnianie dwuskładnikowe” / „2FA”. Wybierz metodę: SMS, token lub aplikacja uwierzytelniająca Google Authenticator lub Microsoft Authenticator (najbezpieczniejsza, trzeba ją wcześniej pobrać na telefon).

Jeśli wybrałeś aplikację uwierzytelniającą - zeskanuj kod QR aplikacją w telefonie **lub** podaj numer telefonu.

Wpisz kod weryfikacyjny.

Od tej pory przy logowaniu podajesz: hasło + jednorazowy kod.

Dobre praktyki haseł: hasła długie i unikalne; nie używaj jednego hasła w wielu serwisach.

Chroń dostęp do urządzeń: blokuj ekran przy odejściu od miejsca pracy, nie zostawiaj nośników bez nadzoru, dbaj o poufność dokumentów.

Korzystaj z bezpiecznych połączeń: używaj VPN w pracy zdalnej, unikaj publicznych Wi-Fi, nie instaluj nieautoryzowanych programów.

Zachowuj czujność wobec wiadomości i linków: sprawdzaj nadawcę, uważaj na błędy językowe, w razie wątpliwości kontaktuj się z IT.

Regularnie wykonuj kopie zapasowe: rób backup ważnych plików, przechowuj kopie bezpiecznie, testuj odtwarzanie danych.

Zgłaszaj incydenty: każde podejrzenie naruszenia zgłaszaj jak najszybciej – szybka reakcja ogranicza szkody.

CHECKLISTA BEZPIECZNEGO WYJAZDU SŁUŻBOWEGO

Przed wyjazdem

- upewnij się, że masz aktualne ubezpieczenie
- zabierz tylko niezbędne dane („need-to-travel”)
- usuń zbędne pliki z laptopa
- wykonaj kopię zapasową ważnych danych
- włącz 2FA czyli uwierzytelnianie dwuskładnikowe – instrukcja na stronie 18
- zaktualizuj system i oprogramowanie
- ustaw automatyczną blokadę ekranu
- ustaw silne hasło do urządzenia
- wyłącz automatyczne łączenie z wi-fi

Sprawdź bezpieczeństwo miejsca podróży (komunikaty na stronie Ministerstwa Spraw Zagranicznych). **Zgłoś wyjazd w systemie Odyseusz** (www.odyseusz.msz.gov.pl) jeśli:

- jest to podróż do kraju o podwyższonym ryzyku
- jest to wyjazd służbowy poza UE
- jest to pobyt w regionach objętych ostrzeżeniami MSZ
- jest to dłuższy pobyt zagraniczny

Dlaczego to ważne?

- ułatwia kontakt służb konsularnych
- przyspiesza pomoc w sytuacji kryzysowej
- zwiększa bezpieczeństwo pracowników i studentów

W trakcie wyjazdu

- korzystaj bezpiecznie z Internetu
- używaj VPN przy pracy z systemami uczelni
- unikaj otwartych sieci wi-fi
- w razie potrzeby korzystaj z hotspotu telefonu
- nie loguj się do systemów na cudzych urządzeniach
- chroń sprzęt i dokumenty (nie zostawiaj laptopa bez nadzoru, nie wkładaj sprzętu do bagażu rejestrowanego, blokuj ekran przy każdej nieobecności, uważaj na „podglądanie przez ramię” w miejscach publicznych)
- zachowaj ostrożność wobec nowych „okazji współpracy”
- nie przekazuj danych służbowych bez uprawnień
- ostrożnie udostępniaj nieopublikowane wyniki badań i świadomie dobieraj zakres ujawnianych danych

W przypadku incydentu zagranicą (np. kradzież laptopa, logowanie przez fałszywe wi-fi w hotelu) natychmiast:

- zabezpiecz konta (zmień hasła, wyloguj sesje)
- zgłoś incydent do działu IT oraz do Inspektora Danych Osobowych UW (abuse@uw.edu.pl; iod@adm.uw.edu.pl)
- zgłoś kradzież lokalnej policji (jeśli dotyczy)
- w razie potrzeby skontaktuj się z konsulem
- udokumentuj zdarzenie

Po powrocie

- zmień hasła do kluczowych systemów
- sprawdź komputer programem antywirusowym
- usuń zbędne dane z urządzenia
- zgłoś ewentualne incydenty lub podejrzenia

DOBRE PRAKTYKI

Bezpieczeństwo na wydziale obejmuje także codzienne praktyki związane z ochroną pomieszczeń, dokumentów, sprzętu oraz informacji. Świadome zachowania istotnie ograniczają ryzyko incydentów.

Kontrola dostępu do pomieszczeń

Zasada: do pomieszczeń wydziału powinny mieć dostęp wyłącznie osoby uprawnione

Dlaczego to ważne:

- ogranicza ryzyko kradzieży sprzętu i dokumentów
- zmniejsza możliwość pozyskania informacji przez osoby postronne
- zwiększa bezpieczeństwo studentów i pracowników

Dobre praktyki:

- zwracaj uwagę na osoby nieznane przebywające na terenie Wydziału, w razie wątpliwości skontaktuj się z portiernią
- jeśli zauważysz zachowanie agresywne lub budzące zagrożenie
- niezwłocznie powiadom Straż Uniwersytecką

Bezpieczeństwo pomieszczeń podczas zajęć

Zasada: w salach zamykanych na klucz podczas zajęć klucz powinien znajdować się w zamku od strony wewnętrznej

Dlaczego to ważne:

- umożliwia szybkie zamknięcie pomieszczenia w sytuacji zagrożenia;
- przyspiesza ewakuację w razie potrzeby
- ogranicza ryzyko wtargnięcia osób nieuprawnionych

Dobre praktyki:

- sprawdź przed zajęciami, czy klucz znajduje się w zamku od wewnętrznej strony drzwi
- upewnij się, że droga ewakuacyjna z sali jest drożna
- w sytuacji zagrożenia stosuj się do poleceń prowadzącego lub służb

Ochrona dokumentów i informacji

Zasada: nie pozostawiaj dokumentów zawierających dane na biurku po zakończeniu pracy

Dlaczego to ważne:

- chroni dane osobowe studentów i pracowników
- zapobiega przypadkowemu ujawnieniu wyników badań lub informacji administracyjnych
- ogranicza ryzyko fotografowania lub kopiowania dokumentów przez osoby postronne

Dobre praktyki:

- przechowuj dokumenty w zamykanych szafach
- ogranicz dostęp do dokumentów wyłącznie do osób uprawnionych
- blokuj komputer przy każdym odejściu od stanowiska pracy

Bezpieczeństwo podczas konsultacji ze studentami

Zasada: spotkania konsultacyjne prowadź w warunkach zapewniających poufność i bezpieczeństwo.

Dlaczego to ważne:

- chroni poufność rozmów
- zwiększa bezpieczeństwo osobiste pracowników i studentów
- ogranicza ryzyko sytuacji konfliktowych

Dobre praktyki:

- unikaj spotkań w całkowicie odosobnionych pomieszczeniach
- w sytuacjach potencjalnie trudnych poinformuj współpracowników o konsultacji
- w razie zagrożenia skontaktuj się z portiernią lub ochroną

Reagowanie na nietypowe sytuacje i zachowania

Zasada: reaguj na wszelkie sytuacje budzące niepokój na terenie budynku

Dlaczego to ważne:

- umożliwia szybkie wykrycie potencjalnych zagrożeń
- zwiększa bezpieczeństwo całej społeczności akademickiej
- pozwala zapobiegać incydentom lub ograniczyć ich skutki

Dobre praktyki:

- nie odpowiadaj na nietypowe prośby osób nieznajomych o informacje dot. funkcjonowania wydziału, o pracowników, doktorantów, studentów
- zwracaj uwagę na osoby poszukujące informacji o pracownikach lub pomieszczeniach
- każde zachowanie budzące niepokój zgłaszaj do dyrektora administracji: dyrektor.administracji.wh@uw.edu.pl

Bezpieczeństwo podczas zajęć

Zasada: stosuj się do poleceń prowadzącego i zasad obowiązujących w sali

Dobre praktyki:

- nie blokuj dróg ewakuacyjnych
- nie manipuluj przy sprzęcie komputerowym
- w sytuacji zagrożenia zachowaj spokój i stosuj się do instrukcji

Bezpieczeństwo podczas pracy w godzinach wieczornych

Jeżeli planujesz pracę w budynku w godzinach wieczornych lub w dni wolne:

- poinformuj portiernię o swojej obecności
- unikaj pracy w całkowicie pustych częściach budynku
- w razie niepokojących sytuacji natychmiast powiadom Straż Uniwersytecką
- zawsze miej przy sobie telefon komórkowy

Ochrona rzeczy osobistych

Zasada: nie pozostawiaj rzeczy bez nadzoru

Dlaczego to ważne:

- na uczelniach zdarzają się kradzieże okazjonalne
- utrata laptopa lub telefonu może oznaczać utratę danych
- pozostawienie plecaka, kurtki bez opieki skutkuje powiadomieniem Straży Uniwersyteckiej

Dobre praktyki:

- miej plecak i sprzęt zawsze w zasięgu wzroku
- nie zostawiaj rzeczy w ogólnodostępnych przestrzeniach
- zabezpiecz urządzenia hasłem lub PIN-em

Bezpieczne korzystanie z komputerów wydziałowych

Zasada: chronić dane logowania do systemów uczelni

Dobre praktyki:

- nie zmieniaj ustawień wi-fi w komputerach wydziałowych
- używaj silnego, unikalnego hasła
- włącz 2FA (uwierzytelnianie dwuskładnikowe), jeśli jest dostępne
- nie udostępniaj nikomu swojego hasła
- wyloguj się z kont na komputerach w salach wydziałowych po zakończeniu pracy

Odpowiedzialne publikowanie w Internecie

Zasada: publikuj wizerunki i informacje z uczelni z rozwagą

Dobre praktyki:

- nie udostępniaj danych innych osób bez zgody
- uważaj na publikowanie zdjęć z zajęć
- nie rozpowszechniaj materiałów dydaktycznych bez zgody

Zgłaszanie usterek technicznych

Każda usterka techniczna może stanowić zagrożenie dla bezpieczeństwa

Zgłaszaj w szczególności:

- uszkodzone drzwi lub zamki; nie działające oświetlenie
- zablokowane drogi ewakuacyjne
- uszkodzone instalacje elektryczne
- wycieki wody lub gazu

Usterki zgłaszaj mailowo lub telefonicznie:

- na portiernię: portiernia.wh@uw.edu.pl; 22 55 20 540
- do dyrektora administracji: dyrektor.administracji.wh@uw.edu.pl; 22 55 20 413.

STOPNIE ALARMOWE

Na stronie Wydziału Historii publikujemy informacje, gdy na terenie kraju wprowadzany jest dany stopień alarmowy. Obserwuj stronę, czytaj informacje.

W czasie podwyższonego poziomu zagrożenia stosuj się do komunikatów UW oraz poleceń Straży Uniwersyteckiej i służb.

Stopnie alarmowe ALFA–BRAVO–CHARLIE–DELTA

- ALFA – wzmożona czujność, zgłaszanie podejrzanych osób/przedmiotów
- BRAVO – dodatkowe kontrole wejść, możliwe ograniczenia dostępu
- CHARLIE – ograniczenie wejść, dyżury, przygotowanie do ewakuacji
- DELTA – ścisłe kontrole osób/pojazdów, możliwe ograniczenia funkcjonowania

Stopnie CRP (cyber)

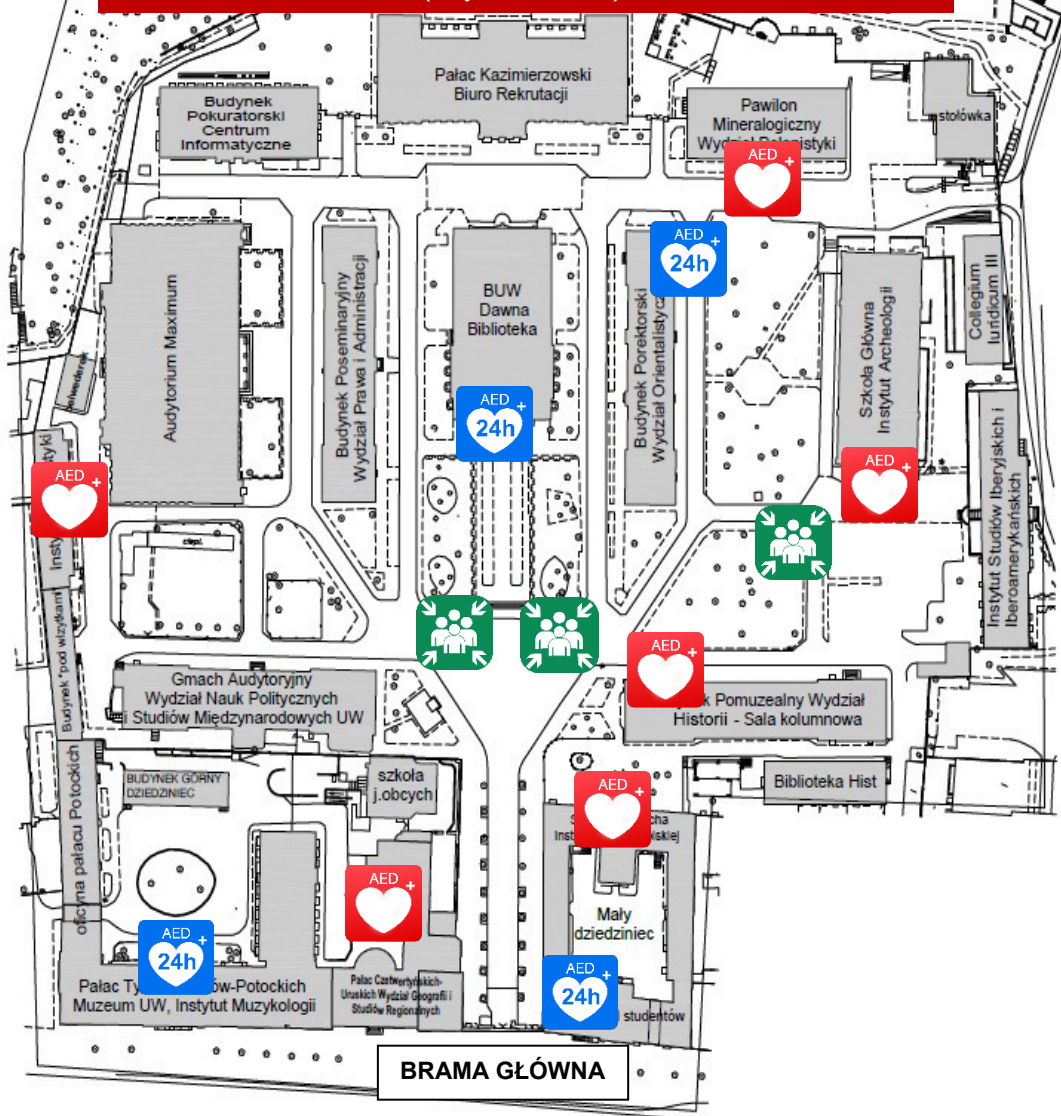
- zachowaj ostrożność w e-mailach i linkach, zgłaszaj podejrzane wiadomości
- możliwe są czasowe ograniczenia dostępu do systemów lub dodatkowe logowanie

ATAK Z POWIETRZA

Atak z powietrza – najważniejsze kroki

- słyszysz niski, buczący dźwięk – działaj natychmiast, nie analizuj
- odejdź od okien (szkło jest szczególnie niebezpieczne)
- szukaj schronienia za dwiema ścianami (korytarz, łazienka bez okien)
- połóż się na podłodze i osłoń głowę rękami
- na zewnątrz – przykucnij nisko i szukaj betonu/zagłębienia terenu
- nie nagrywaj; zostań w schronieniu do odwołania zagrożenia (co najmniej kilka minut ciszy)
- jeśli możesz, miej na sobie buty (szkło i odłamki)

Kampus centralny UW
miejsca zbiórki do ewakuacji oraz lokalizacje defibrylatorów AED
(w tym AED 24h).



defibrylator dostępny całą dobę



defibrylator



miejsce zbiórki do ewakuacji

Ważne numery telefonów:

Numer alarmowy: 112

Straż Uniwersytecka: 22 55 22 112

Portiernia WH: 22 55 20 540

Dyrektor administracji: 22 55 20 413

Dziekanat: 22 55 20 415

Bezpieczeństwo to wspólna odpowiedzialność.

Bezpieczeństwo na uczelni
nie zależy wyłącznie od służb i procedur.
W dużej mierze opiera się na czujności i odpowiedzialności
całej społeczności akademickiej.

Reaguj na sytuacje budzące niepokój.
Zgłaszaj zagrożenia i usterki.
Stosuj się do komunikatów uczelni i służb.
Dbaj o bezpieczeństwo swoje i innych.

Tvoja reakcja może zapobiec poważnemu zdarzeniu.