UNIWERSYTET WARSZAWSKI

Inspektor Ochrony Danych

IOD-042-04/2026

ZASADY CYBERHIGIENY

Poradnik dla społeczności akademickiej Uniwersytetu Warszawskiego

Warszawa – 19.02.2026

I. Wprowadzenie

Rozwój technologii cyfrowych sprawił, że dane stały się jednym z najcenniejszych zasobów organizacji i osób prywatnych. W dobie cyfryzacji i powszechnego przetwarzania informacji zagadnienie ochrony informacji nabiera coraz większego znaczenia. Codziennie przetwarzamy i przekazujemy ogromne ilości danych – zarówno w życiu prywatnym, jak i zawodowym. Niestety, wraz z tym rośnie ryzyko **naruszeń bezpieczeństwa informacji**.

Dane przechowujemy systemach informatycznych, w chmurze, na urządzeniach mobilnych czy w poczcie elektronicznej. Wraz ze wzrostem ilości danych rośnie także liczba zagrożeń.

Cyberhigiena oznacza codzienne praktyki i nawyki, które ograniczają ryzyko naruszeń bezpieczeństwa. Nie polega ona wyłącznie na stosowaniu technologii, lecz przede wszystkim na świadomym zachowaniu użytkowników.

Celem niniejszego poradnika jest przedstawienie podstawowych pojęć, zagrożeń oraz dobrych praktyk związanych z ochroną danych i bezpieczeństwem cyfrowym.

II. Podstawowe definicje

Cyberbezpieczeństwo – działania, technologie i procedury chroniące systemy oraz dane przed nieuprawnionym dostępem, utratą lub zakłóceniem działania.

Cyberhigiena – zbiór dobrych praktyk związanych z bezpiecznym korzystaniem z technologii informatycznych, obejmujący m.in. zarządzanie hasłami, aktualizacje systemów, ochronę danych oraz ostrożność wobec zagrożeń.

Dane – to wszelkie informacje zapisane w dowolnej formie, które opisują osoby, zdarzenia, procesy lub wyniki pracy i mogą być przechowywane, przetwarzane oraz udostępniane.

Obejmują one m.in.:

- dane osobowe (np. imię, nazwisko, adres e-mail),
- dane badawcze (np. wyniki pomiarów, ankiety, modele, artykuły przed publikacją),
- dane dydaktyczne (np. materiały zajęciowe, oceny),
- dane administracyjne i finansowe (np. dokumenty, umowy),
- dane techniczne (np. logi systemowe, identyfikatory użytkowników, konfiguracje).

Najprościej: dane to informacje, które coś opisują i mają wartość – organizacyjną, naukową lub prawną – dlatego wymagają odpowiedniej ochrony i właściwego zarządzania.

Incydent bezpieczeństwa – to każde zdarzenie, które może naruszyć poufność, integralność lub dostępność danych albo systemów informatycznych. Nie musi oznaczać udanego ataku – incydentem może być również próba naruszenia lub sytuacja stwarzająca ryzyko.

Przykłady incydentów:

- nieautoryzowany dostęp do systemu;
- utrata lub kradzież urządzenia;
- wysłanie e-maila z danymi do niewłaściwego odbiorcy;
- infekcja złośliwym oprogramowaniem;
- ujawnienie danych w Internecie;
- podejrzana wiadomość phishingowa;
- awaria systemu wpływająca na dostęp do danych.

Skutki incydentów mogą obejmować straty finansowe, zakłócenia pracy organizacji, utratę reputacji, konsekwencje prawne oraz ryzyko kradzieży tożsamości.

Warto podkreślić, że wiele incydentów wynika z błędów ludzkich i nieświadomych działań.

Poufność, integralność, dostępność – trzy podstawowe cele ochrony danych: poufność (kto widzi), integralność (czy dane są poprawne), dostępność (czy można z nich korzystać).

III. Najpowszechniejsze cyberzagrożenia

Phishing

to metoda oszustwa polegająca na podszywaniu się pod zaufane instytucje lub osoby w celu wyłudzenia informacji, takich jak dane logowania, dane osobowe czy informacje finansowe. Ataki najczęściej przybierają formę wiadomości e-mail zawierających link prowadzący do fałszywej strony logowania lub załącznik ze złośliwym oprogramowaniem.

Celem phishingu jest skłonienie odbiorcy do wykonania działania bez dokładnej weryfikacji, np. zalogowania się do systemu uczelnianego, potwierdzenia danych, pobrania pliku lub dokonania płatności. Fałszywe wiadomości są często przygotowane tak, aby wyglądały wiarygodnie i nawiązywały do bieżących spraw służbowych.

Typowe cechy phishingu:

- wywieranie presji czasu lub konieczność natychmiastowego działania,
- prośba o podanie danych, wykonanie płatności lub kliknięcie w link,
- adres nadawcy podobny do prawdziwego, lecz zmodyfikowany,
- komunikaty odwołujące się do strachu, pilności lub konsekwencji braku reakcji.

W przypadku podejrzenia phishingu nie należy klikać w linki ani nie otwierać załączników oraz zweryfikować wiadomość poprzez oficjalny kanał komunikacji lub kontakt z działem IT.

Więcej:
https://odo.uw.edu.pl/2025/05/09/uwaga-phishing-komunikat-iod/
https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/07/Phishing.pdf
https://cert.pl/posts/2025/09/analiza-adresow-stron/
https://cert.pl/posts/2023/04/phishing-webmail/

Malware

(złośliwe oprogramowanie) to program lub kod instalowany na urządzeniu bez wiedzy lub świadomej zgody użytkownika, którego celem jest naruszenie bezpieczeństwa systemu lub danych. Malware może działać w ukryciu, zbierać informacje, zakłócać pracę komputera albo umożliwiać przeprowadzenie kolejnych ataków.

Do najczęstszych funkcji złośliwego oprogramowania należą kradzież danych logowania, monitorowanie aktywności użytkownika, przejmowanie kontroli nad urządzeniem, szyfrowanie plików, a także wykorzystywanie komputera do rozsyłania spamu lub ataków na inne systemy.

Infekcja może nastąpić m.in. po otwarciu podejrzanego załącznika, kliknięciu w niebezpieczny link, instalacji nieautoryzowanego programu lub podłączeniu zainfekowanego nośnika danych. Malware może prowadzić do wycieku danych, utraty wyników badań czy zakłócenia pracy systemów dydaktycznych i administracyjnych.

Ochrona przed malware opiera się na aktualizowaniu oprogramowania, korzystaniu z narzędzi zabezpieczających, ostrożności wobec plików i linków oraz ograniczaniu instalacji oprogramowania do sprawdzonych źródeł.

Ransomware

to rodzaj złośliwego oprogramowania, które blokuje dostęp do danych lub szyfruje pliki zawierające dane, a następnie żąda okupu za ich odzyskanie. Po infekcji użytkownik często traci możliwość otwarcia dokumentów, a na ekranie pojawia się komunikat z instrukcją zapłaty.

Ataki ransomware mogą rozpocząć się od kliknięcia w złośliwy załącznik, link phishingowy, instalacji nieautoryzowanego programu lub wykorzystania nieaktualnego oprogramowania. W środowisku uczelni skutkiem może być zablokowanie materiałów dydaktycznych, wyników badań, dokumentacji projektowej czy systemów administracyjnych, co prowadzi do poważnych zakłóceń pracy.

Zapłacenie okupu nie gwarantuje odzyskania danych i może zachęcać sprawców do dalszych ataków. Dlatego **kluczowe znaczenie ma profilaktyka**: regularne aktualizacje, ostrożność wobec wiadomości i linków, ograniczanie uprawnień oraz wykonywanie kopii zapasowych, które umożliwiają odtworzenie danych bez konieczności płacenia.

Więcej: https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

Smishing

(SMS phishing) to forma oszustwa polegająca na wyłudzaniu informacji za pomocą wiadomości SMS lub komunikatorów internetowych. Osoba atakująca wysyła wiadomość, podszywając się pod zaufaną instytucję, np. firmę kurierską, bank, operatora płatności czy administratora systemu uczelnianego.

Wiadomość zwykle zawiera informację o konieczności dopłaty do przesyłki, blokadzie konta, pilnej weryfikacji danych lub rzekomej nagrodzie. Jej celem jest skłonienie odbiorcy do kliknięcia w link prowadzący do fałszywej strony, na której proszony jest o podanie danych logowania, danych osobowych lub informacji płatniczych.

Podstawową zasadą bezpieczeństwa jest nieklikanie w linki z nieoczekiwanych wiadomości oraz weryfikowanie informacji bezpośrednio na oficjalnej stronie instytucji lub poprzez kontakt z działem IT. Wiadomości wywołujące presję czasu lub wymagające natychmiastowego działania należy traktować ze szczególną ostrożnością.

Więcej: https://cert.pl/baza-wiedzy/falszywe-smsy/

Vishing

(voice phishing) to forma oszustwa wykorzystująca rozmowy telefoniczne. Polega na tym, że osoba dzwoniąca podszywa się pod zaufaną instytucję lub współpracownika — np. pracownika banku, działu IT, kuriera, firmy informatycznej czy przełożonego — i próbuje nakłonić rozmówcę do ujawnienia informacji lub wykonania określonej czynności.

Celem vishingu może być uzyskanie danych logowania, kodów autoryzacyjnych, informacji o systemach uczelni, instalacja oprogramowania lub wykonanie przelewu. Oszuści często wywierają presję czasu, odwołują się do autorytetu („dział bezpieczeństwa", „pilna sprawa od kierownika") albo straszą konsekwencjami, aby skłonić do szybkiego działania bez weryfikacji.

Podstawową zasadą jest ograniczone zaufanie: wrażliwych danych, haseł ani kodów **nie należy** przekazywać telefonicznie. W przypadku nietypowej prośby należy zakończyć rozmowę i samodzielnie skontaktować się z daną osobą lub jednostką poprzez oficjalny kanał.

Więcej: https://odo.uw.edu.pl/2025/05/15/uwaga-vishing-komunikat-iod/

IV. Podstawowe zasady cyberhigieny

Aktualizuj oprogramowanie i korzystaj ze sprawdzonych zabezpieczeń

Regularne aktualizacje systemów operacyjnych, aplikacji oraz oprogramowania antywirusowego eliminują wykryte luki bezpieczeństwa i znacząco zmniejszają ryzyko incydentów. Nie należy odkładać instalacji poprawek – wiele ataków wykorzystuje znane, niezałatane podatności.

Stosuj silne, unikalne hasła oraz uwierzytelnianie dwuskładnikowe (2FA)

Hasła powinny być długie, unikalne i trudne do odgadnięcia. Nie zaleca się używania tych samych haseł w różnych serwisach. Rekomendowane jest korzystanie z menedżera haseł oraz włączanie uwierzytelniania dwuskładnikowego wszędzie tam, gdzie jest to możliwe.

Poradniki:

https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/03/praca-zdalna-poradnik.pdf
https://cert.pl/bezpieczne-hasla/

Chroń informacje przed nieuprawnionym dostępem

Podczas każdej nieobecności przy stanowisku pracy należy blokować ekran komputera. Należy również dbać o poufność dokumentów w wersji papierowej i elektronicznej oraz nie pozostawiać nośników danych bez nadzoru.

Poradnik:

https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/03/bezpieczne-korzystanie-z-urz%C4%85dze%C5%84-IT.pdf

Korzystaj wyłącznie z bezpiecznych połączeń i zaufanych urządzeń

W pracy zdalnej należy korzystać z uczelnianego VPN oraz zabezpieczonej sieci Wi-Fi. Należy unikać logowania do systemów służbowych z publicznych, niezabezpieczonych sieci oraz instalowania nieautoryzowanego oprogramowania na sprzęcie służbowym.

Poradnik:

https://odo.uw.edu.pl/wp-content/uploads/sites/10/2021/02/DOZI.W.01.2021.pdf

Udostępniaj informacje wyłącznie osobom upoważnionym

Należy stosować zasadę minimalnego dostępu, przekazując dane wyłącznie osobom, które faktycznie potrzebują ich do realizacji obowiązków służbowych. Przed wysłaniem wiadomości warto każdorazowo sprawdzić poprawność adresata, szczególnie przy korespondencji zawierającej dane wrażliwe.

Zachowuj czujność wobec wiadomości i linków

Należy zwracać uwagę na nietypowe wiadomości e-mail, prośby o pilne działanie, błędy językowe czy podejrzane załączniki. Przed kliknięciem w link lub otwarciem pliku należy zweryfikować nadawcę. W przypadku wątpliwości należy skontaktować się z działem IT.

Poradniki:

https://odo.uw.edu.pl/2025/05/30/jak-bezpiecznie-korzystac-z-poczty-elektronicznej/
https://odo.uw.edu.pl/wp-content/uploads/sites/10/2020/12/wskazowki-dot.-prowadzenia-korespondencji.pdf
https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf

Publikuj odpowiedzialnie w Internecie

Udostępniając informacje w mediach społecznościowych i na stronach internetowych, należy zachować rozwagę. Wskazane jest unikanie publikowania danych mogących ułatwić potencjalne ataki, np. szczegółów dotyczących infrastruktury, procedur czy harmonogramów.

Szyfruj dane i nośniki przenośne

Przy pracy z danymi wrażliwymi należy stosować szyfrowanie plików oraz zabezpieczenia nośników zewnętrznych, takich jak pendrive'y i dyski przenośne. Utrata niezabezpieczonego nośnika może skutkować naruszeniem bezpieczeństwa danych.

Regularnie wykonuj kopie zapasowe

Wskazane jest tworzenie kopii zapasowych istotnych plików i dokumentów. Kopie powinny być przechowywane w bezpiecznym miejscu oraz okresowo weryfikowane pod kątem możliwości odtworzenia danych.

Regularnie uczestnicz w szkoleniach

Bierz udział w szkoleniach i zapoznawaj się z komunikatami bezpieczeństwa.

Szkolenia: https://odo.uw.edu.pl/szkolenia/

Niezwłocznie zgłaszaj incydenty bezpieczeństwa

Każde podejrzenie naruszenia bezpieczeństwa, takie jak utrata urządzenia, podejrzane logowanie czy nieautoryzowany dostęp do danych, należy niezwłocznie zgłosić właściwej jednostce. Szybka reakcja pozwala ograniczyć skalę potencjalnych szkód.

Zgłaszanie naruszeń: https://odo.uw.edu.pl/zglaszanie-naruszen-ochrony-danych/

Kontakt: **iod@adm.uw.edu.pl**