Akademia Muzyczna
im. Ignacego Jana Paderewskiego w Poznaniu

Regulamin ochrony danych osobowych

Co każdy pracownik wiedzieć powinien

(wyciąg z Polityki Ochrony Danych Osobowych)

Poniższe informacje mają na celu przedstawienie w przystępny sposób podstawowej terminologii oraz zasad ochrony danych osobowych i bezpieczeństwa informacji.

Przestrzeganie poniższych reguł jest obowiązkiem każdego pracownika lub współpracownika Akademii Muzycznej im. I.J. Pendereckiego, mającego lub mogącego mieć do czynienia z danymi osobowymi.
Naruszenie poniższych zasad zostanie uznane za niedotrzymanie zobowiązań umownych.
Zapoznaj się z nimi, aby wiedzieć po co i w jaki sposób chronić dane osobowe.

Spis treści

Słowniczek 2
Obowiązkowe zasady postępowania 4
Najczęściej występujące zagrożenia 7
Zalecenia dla pracowników dydaktycznych 10
Postępowanie w razie wystąpienia zagrożenia 12
Zgłaszanie naruszeń 13
Bezpieczeństwo danych podczas pracy online 14

Inspektor Ochrony Danych
Jędrzej Dzida

Słowniczek

RODO—*rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE*

Dane osobowe *- oznaczają informacje o zidentyfikowanej (np. Jan Nowak, ul. Hoża 5/12, 02-512 Warszawa) lub możliwej do zidentyfikowania osobie fizycznej (np. osoba o numerze PESEL 91121720152);*
możliwa do zidentyfikowania osoba fizyczna to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, dane o lokalizacji, identyfikator internetowy (adres poczty elektronicznej, nick na forum) lub jeden bądź kilka szczególnych czynników określających: fizyczną (np. skan tęczówki oka lub odcisk palca), fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (np. dyrektor teatru, członek zarządu, radny urzędu gminy).

Administrator danych *- rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną, które samodzielnie lub wspólnie z innymi decydują o celach i sposobach przetwarzania danych osobowych, np. adwokat prowadzący własną kancelarię, spółka z ograniczoną odpowiedzialnością, stowarzyszenie, biblioteka, szkoła lub przedszkole. Administratorem jest uczelnia a nie jej rektor, szkoła a nie dyrektor szkoły.*

Przetwarzanie danych osobowych *- oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany (systemy informatyczne) lub niezautomatyzowany (forma papierowa), w tym przede wszystkim: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (np. zapisanie danych na kartce papieru, przechowywanie kwestionariuszy osobowych, archiwizacja formularzy kontaktowych, zapisanie danych na pendrivie, przesłanie kopii umów, wysłanie marketingu elektronicznego).*

Organ nadzorczy (Urząd Ochrony Danych Osobowych - UODO) – *niezależny organ publiczny odpowiedzialny za monitorowanie stosowania przepisów o ochronie danych osobowych. Urzędem kieruje Prezes UODO.*

Podmiot przetwarzający (procesor) *- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu i na rzecz administratora. Procesorem będzie więc podmiot zewnętrzny, który zgodnie z zawartą z administratorem* ***umową o powierzeniu danych do przetwarzania*** *i tylko w zakresie w niej określonym, wspiera administratora w określonych sferach jego działalności, przetwarzając w jego imieniu dane osobowe, np. firma hostingowa, biuro księgowe, firmy drukujące lub obsługujące korespondencję otrzymywaną od klientów, firmy archiwizujące dokumenty, firmy zajmujące się badaniami opinii klientów, partnerzy świadczący usługi techniczne (np. rozwijanie i utrzymywanie systemów informatycznych i serwisów internetowych).*

Inspektor ochrony danych (IOD) *– oznacza osobę wyznaczoną przez administratora danych lub podmiot przetwarzający, która monitoruje i weryfikuje zakres przestrzegania przepisów o ochronie danych osobowych oraz doradza w tym zakresie i wydaje odpowiednie rekomendacje.*

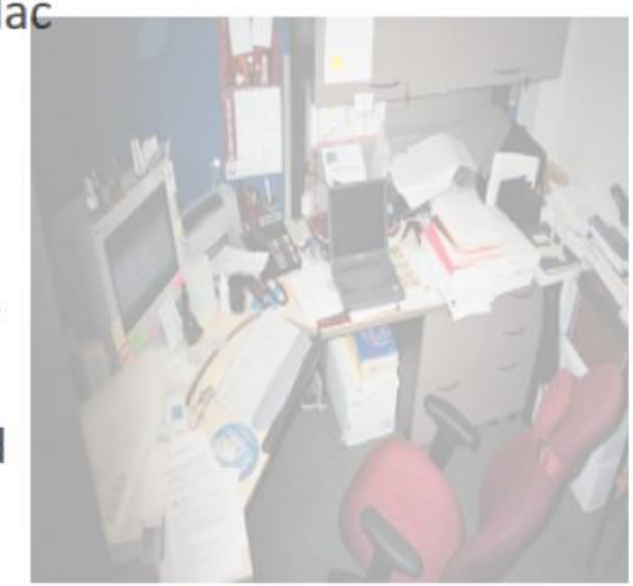
Upoważnienie do przetwarzania danych *- rozumie się przez to upoważnienie nadawane przez administratora danych lub podmiot przetwarzający, wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym upoważnieniu.*

Warunkiem otrzymania upoważnienia *jest udział w szkoleniu prowadzonym przez Inspektora Ochrony Danych nt. zasad ochrony danych osobowych (dla pracowników etatowych) lub zapoznanie się z Regulaminem ochrony danych, potwierdzone własnoręcznym podpisem (dla kontrahentów i osób współpracujących)*

Obowiązkowe zasady postępowania (nakazy)

Polityka zarządzania hasłami

należy pamiętać o konieczności logowania się do systemu, aplikacji czy programu przy pomocy własnego loginu i hasła. Hasło powinno składać się przynajmniej z 8 znaków (dużych i małych liter, cyfr i znaków specjalnych) i powinno być zmieniane co najmniej raz na 90 dni.



Polityka czystego biurka

należy pamiętać o konieczności przechowywania wszelkich nośników danych osobowych (np. dokumentów) poza zasięgiem wzroku i zasięgiem ręki osób postronnych, a także o przechowywaniu ich pod kluczem.

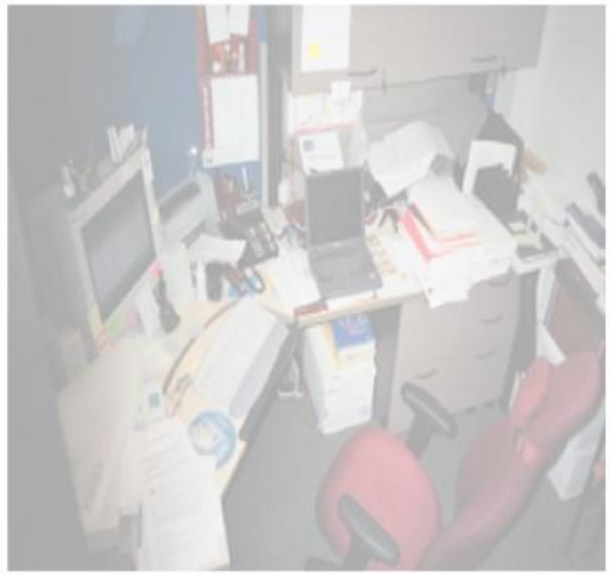
Polityka bezpiecznego ekranu

należy pamiętać o konieczności blokowania komputerów przed każdorazowym, nawet chwilowym opuszczeniem stanowiska pracy (np. skrót klawiszowy WIN+L). Dodatkowo należy uniemożliwiać wgląd w treści wyświetlane na monitorach osobom nieupoważnionym – choćby poprzez odpowiednie ustawienie ekranu lub stosowanie filtrów prywatyzujących.

Obowiązkowe zasady postępowania (nakazy)

Polityka bezpiecznego druku

należy pamiętać o konieczności odbierania wszelkich wydruków z urządzeń drukujących niezwłocznie po ich wydrukowaniu.



Procedura bezpiecznego niszczenia

należy pamiętać o konieczności niszczenia dokumentów zawierających dane osobowe z wykorzystaniem niszczarek lub pojemników do utylizacji dokumentacji zawierającej dane osobowe.

Procedura korzystania z urządzeń mobilnych

należy pamiętać o konieczności zabezpieczania sprzętu informatycznego (laptopy, smartfony, tablety, pendrive'y) przed wyniesieniem ich poza obszar pracy (obszar przetwarzania danych) – hasłem, PIN-em, przy zastosowaniu technologii biometrycznych oraz szyfrowaniu zawartych na nich danych.

Obowiązkowe zasady postępowania (nakazy)

Procedura korzystania z Internetu

należy pamiętać o zakazie stosowania zapamiętywania haseł w przeglądarkach internetowych oraz historii wyszukiwania – okresowo należy czyścić historię przeglądania lub wyłączyć jej zapamiętywanie.

Procedura korzystania z poczty elektronicznej 1

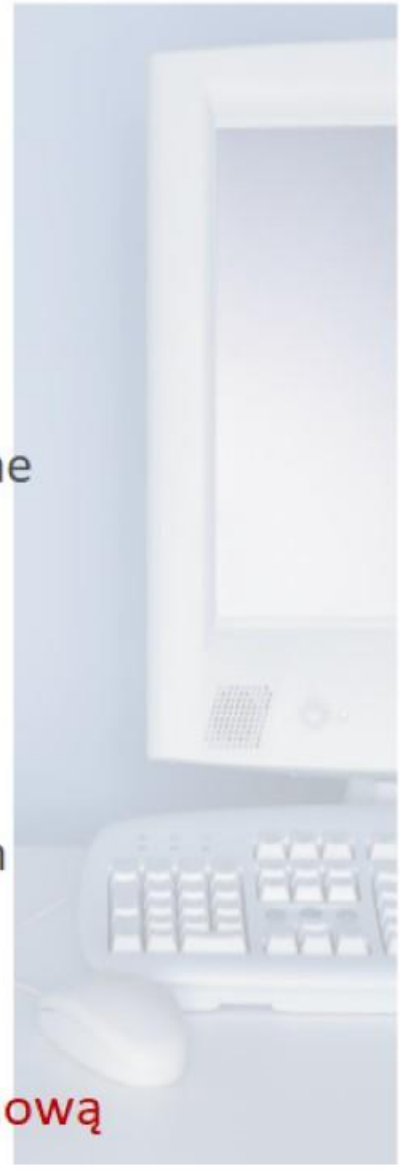
należy pamiętać, że wysyłanie wiadomości służbowych powinno być wykonywane tylko ze służbowej poczty elektronicznej i tylko na służbowe skrzynki mailowe.

Procedura korzystania z poczty elektronicznej 2

należy pamiętać o weryfikacji adresów mailowych w procesie wysyłania tak, by adresacja była prawidłowa – w szczególności należy weryfikować opcje kopia ukryta/ kopia jawna. Dodatkowo nie wolno korzystać z odnośników znajdujących się w mailach nieznanego pochodzenia.

PAMIĘTAJ:

wszelkie informacje przesyłane pocztą służbową stanowią tajemnicę firmową



Najczęściej występujące zagrożenia

Opuszczenie stanowiska pracy

i pozostawienie aktywnej aplikacji lub systemu operacyjnego, umożliwiające dostęp do bazy danych osobowych osobie nieuprawnionej.

Dopuszczenie do korzystania z systemu

operacyjnego lub aplikacji umożliwiających dostęp do bazy danych osobowych przez jakiekolwiek osoby inne niż osoba, której identyfikator został przydzielony.

Pozostawienie w miejscu widocznym

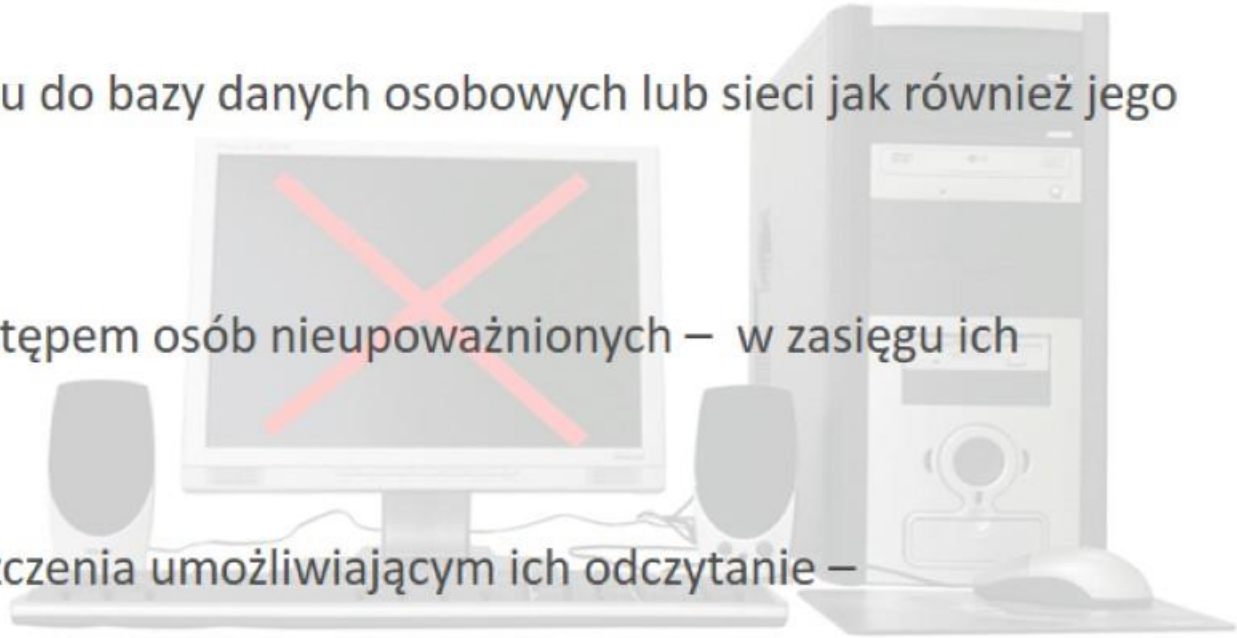
lub oczywistym zapisanego hasła dostępu do bazy danych osobowych lub sieci jak również jego współdzielenie z osobami trzecimi.

Przechowywanie dokumentów

niewłaściwie zabezpieczonych przed dostępem osób nieupoważnionych – w zasięgu ich wzroku lub rąk.

Wyrzucanie dokumentów

do zwykłych śmietników w stopniu zniszczenia umożliwiającym ich odczytanie – niekorzystanie z niszczarek.



Najczęściej występujące zagrożenia

Dopuszczanie
aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe – niezapewnienie polityki czystego ekranu.

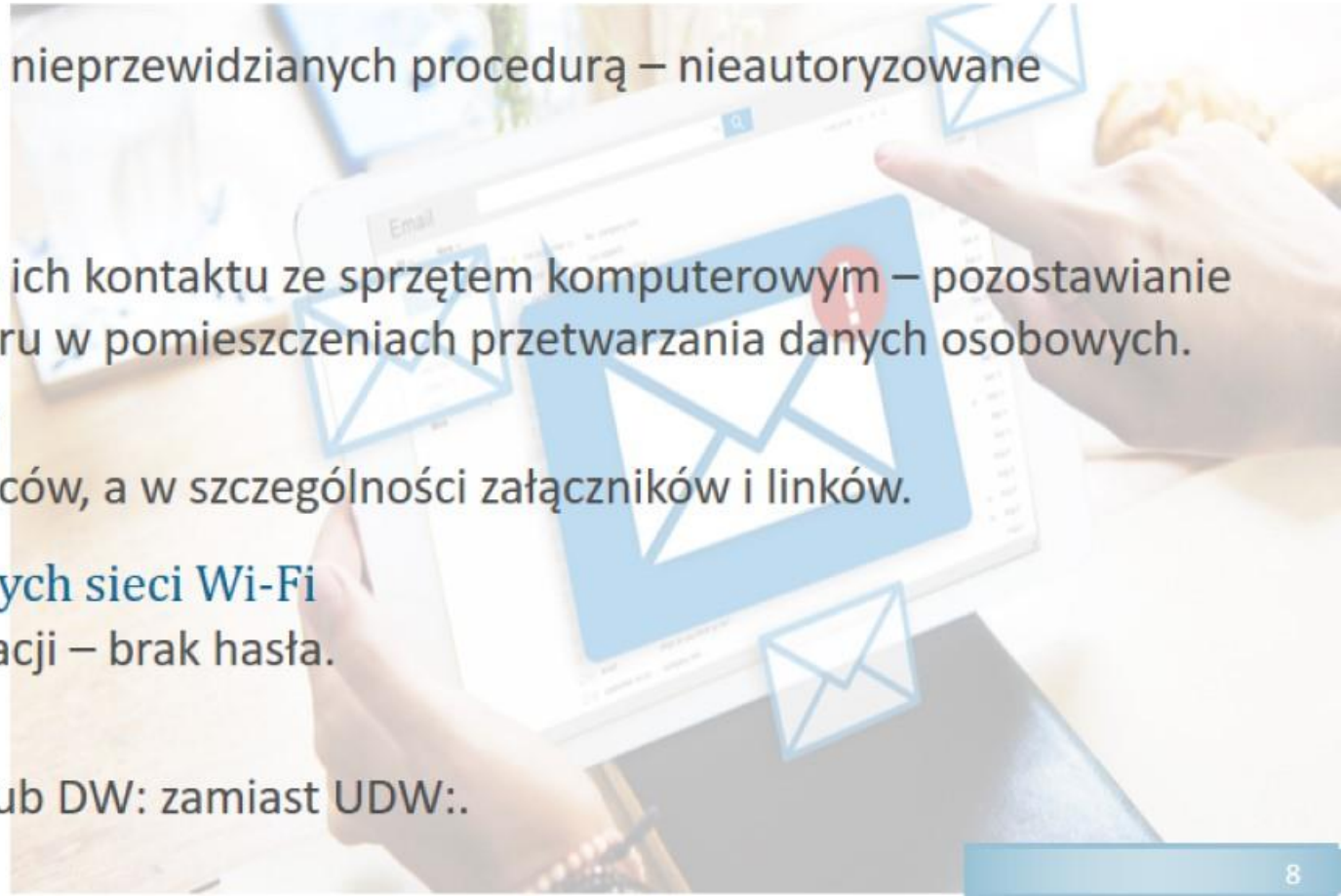
Sporządzanie kopii danych
na nośnikach danych w sytuacjach nieprzewidzianych procedurą – nieautoryzowane wynoszenie danych osobowych.

Wpuszczanie do pomieszczeń
osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym – pozostawianie osób nieupoważnionych bez nadzoru w pomieszczeniach przetwarzania danych osobowych.

Otwieranie poczty elektronicznej
pochodzącej od nieznanych nadawców, a w szczególności załączników i linków.

Korzystanie z publicznie dostępnych sieci Wi-Fi
które nie posiadają żadnej autoryzacji – brak hasła.

Wysłanie mailingu masowego
z wpisaniem adresów w pole DO: lub DW: zamiast UDW:.



W razie wystąpienia któregokolwiek z powyższych zdarzeń, należy niezwłocznie skontaktować się z przełożonym, IOD lub z najwyższym kierownictwem uczelni i poinformować o zdarzeniu.

Zalecenia dla pracowników dydaktycznych

Nie wolno

zbierać od studentów dodatkowych danych osobowych, oprócz tych, które są dostępne w systemie (np. prywatnych numerów telefonów - oprócz sytuacji, gdy student wyraził zgodę na przekazanie numeru — np.. poprzez wykonanie ze swojego numeru, połączenia do pedagoga).

Nie wolno

podawać zbiorowej informacji o ocenach, w wykazach zawierających imię i nazwisko studenta (zamiast tego, należy podać nr albumu).

Zabronione jest

tworzenie i pozostawianie bez nadzoru wszelkiego rodzaju list, wykazów i zestawień studentów, zawierających dane osobowe.

Zabronione jest

wykorzystywanie prywatnych skrzynek poczty elektronicznej do kontaktów służbowych.

Obowiązkowo

posiadane w formie elektronicznej dane osobowe zabezpieczyć osobnym hasłem lub zaszyfrować.

Organizując

konferencje, konkursy i inne eventy podczas których zbierane będą dane osobowe (np. poprzez formularze zgłoszeniowe), proszę o wcześniejszy kontakt (adres poniżej), w celu przygotowania niezbędnej dokumentacji związanej z RODO.

W przypadku wątpliwości

proszę pisać na adres: jdzida@amuz.edu.pl

Postępowanie w razie wystąpienia zagrożenia

Zabezpieczyć pozostałe dane osobowe
jeżeli zdarzenie stwarza taką możliwość.

Niezwłocznie zgłosić zdarzenie
bezpośredniemu przełożonemu, do działu IT i do IOD.

Ustalić okoliczności naruszenia
ochrony danych osobowych.

Sporządzić dokumentację
naruszenia (notatkę).

Zastosować działania zapobiegawcze
by nie doszło ponownie do zdarzenia.

Współpracować z IOD
lub przedstawicielami organu nadzorczego.

Zgłaszanie naruszeń

Naruszenie bezpieczeństwa może polegać np.: na próbie fizycznego dostępu do danych osobowych przez osobę nieuprawnioną (np. kradzież dokumentów), dostępie do systemu informatycznego zawierającego dane osobowe i ich nieuprawniona zmiana lub zagubieniu pendrive'a z danymi i brak dostępu do nich.

Zgłoszenie naruszenia ochrony danych osobowych powinno być dokonane **natychmiast** po zauważeniu, nie później jednak niż 12 godzin od podejrzenia naruszenia.

Kontakt w razie incydentu

helpdesk@amuz.edu.pl

oraz do swojego przełożonego

Bezpieczeństwo danych podczas pracy online

1. Zanim przystąpisz do pracy, wydziel sobie odpowiednią przestrzeń tak, aby ewentualne osoby postronne, nie miały dostępu do dokumentów, nad którymi pracujesz (członkowie rodziny nie są osobami upoważnionymi do przetwarzania danych).
2. Wykorzystuj do pracy zdalnej komputer służbowy przygotowany specjalnie do tego celu przez dział IT.
3. Jeżeli używasz komputera prywatnego, przygotuj go do pracy zgodnie z zaleceniami działu IT (nie używaj np. komputera do gier).
4. Upewnij się, że twój komputer ma niezbędne aktualizacje systemu operacyjnego, oprogramowania oraz systemu antywirusowego.
5. Nie instaluj dodatkowych aplikacji i oprogramowania, niezgodnych z procedurą bezpieczeństwa Akademii.
6. Odchodząc od stanowiska pracy każdorazowo blokuj urządzenie, na którym pracujesz.

Bezpieczeństwo danych podczas pracy online

7. Nie używaj tych samych haseł w różnych systemach informatycznych. Dostosuj złożoność haseł odpowiednio do zagrożeń.
8. Szyfruj dyski twarde w komputerach przenośnych.
9. Po zakończonej pracy zamykaj komputer (pamiętaj o “zamykaniu” nie “usypianiu” czy “hibernowaniu”).
10. Nie loguj się do systemów informatycznych uczelni w przypadkowych miejscach, lub do publicznych niezabezpieczonych sieci Wi-Fi.
11. Unikaj wchodzenia na nieznane czy przypadkowe strony internetowe.
12. Nie otwieraj załączników oraz nie wykorzystuj linków dostarczanych poprzez korespondencję elektroniczną z nieznanych źródeł.

Bezpieczeństwo danych podczas pracy online

13. Wykonuj regularne kopie zapasowe.
14. Szyfruj dane osobowe przesyłane pocztą elektroniczną.
15. Korzystaj ze sprawdzonego oprogramowania do szyfrowania e-maili lub nośników danych.
16. Przy pracy zdalnej korzystaj z szyfrowanego połączenia VPN.
17. Nie umieszczaj w komputerze przypadkowo znalezionych nośników USB. Może znajdować się na nich złośliwe oprogramowanie.
18. Podejmij szczególne środki, aby urządzenia z których korzystasz podczas pracy, (szczególnie te wykorzystywane do przenoszenia danych, jak np. dyski zewnętrzne), były szyfrowane i nie zostały zgubione.