Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych

w

Spółce Zakład Mechaniczny

„BUMAR-MIKULCZYCE" S.A.

w Zabrzu

Z DNIA 15.01.2021 r.

Pieczęć:	ZAKŁAD MECHANICZNY "BUMAR-MIKULCZYCE" Spółka Akcyjna 41-807 Zabrze, ul. Handlowa 2 tel. +48 32 373-86-00 do 699 fax +48 32 271-37-42 Regon 271830823 NIP 648-10-00-642
Zatwierdził:	**Data:**
PREZES ZARZĄDU DYREKTOR NACZELNY Tomasz Polus	15.01.2021 r.

Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych

Spis treści

Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych

I. Wstęp

Instrukcja Zarządzania Systemem Informatycznym została opracowana zgodnie z Rozporządzeniem 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 (ogólne rozporządzenie o ochronie danych) oraz wymaganiami określonymi w § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 nr 100 poz. 1024).

Instrukcja stanowi zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych Zakładu Mechanicznego „BUMAR-MIKULCZYCE" S.A z siedzibą w Zabrzu przy ul. Handlowej 2, 41-800.

II. Definicje

1. **Polityka** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych.
2. **Instrukcja** - rozumie się przez to Instrukcję Zarządzania Systemem Informatycznym.
3. **Administrator Danych Osobowych (ADO)** – Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A. z siedzibą w Zabrzu (41–807) przy ul. Handlowej 2 NIP: 6481000642.
4. **Inspektor Ochrony Danych (IOD)** – osoba powołana pisemnie przez ADO, która w jego imieniu sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych oraz wypełnia inne zadania opisane w art. 39 RODO.
5. **Administrator systemu** - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.
6. **Dane osobowe (dane)** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
7. **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
8. **Użytkownik** – osoba posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych lub zleceniem.
9. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów informacyjnych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
10. **Nośnik danych** – nośnik służący do zapisu i przechowywania informacji, np. płyta CD, płyta DVD, pendrive, dysk twardy.
11. **Nośnik wielokrotnego użytku -** płyta CD-RW, płyta DVD-RW, pendrive, dysk twardy.
12. **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela podmiotu mającego siedzibę w państwie trzecim; inny podmiot, któremu na drodze umowy powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

13. **Konto zwykłe** – konto, którego użytkownik posiada dostęp jedynie do niezbędnych danych umożliwiających wykonywanie powierzonych mu obowiązków służbowych.
14. **Konto uprzywilejowane** – konto, którego użytkownik posiada szeroki dostęp do infrastruktury IT oraz do krytycznych zasobów Zakładu (tj.: serwery, firewalle, rutery, macierze, bazy danych, systemy plików, kontrolery domen, materiały stanowiące własność intelektualną chronioną prawami autorskimi, kody źródłowe, ważne i poufne dane, systemy dostępu, itp.).

III. Polityka kluczy

1. Ogólne zasady

a. Polityka kluczy obejmuje pomieszczenia Zakładu Mechanicznego „BUMAR-MIKULCZYCE" S.A. z siedzibą w Zabrzu (41 – 807) przy ul. Handlowej 2.

2. Nadawanie upoważnień

a. Upoważnienia do pobierania kluczy do pomieszczeń mają wyłącznie osoby upoważnione przez bezpośrednich przełożonych.
b. Udzielenie/anulowanie upoważnienia wymaga wprowadzenia osoby do ewidencji, prowadzonej w postaci Matrycy uprawnień.

3. Wydawanie i zdawanie kluczy w siedzibie

a. Klucze do budynku są w posiadaniu wyznaczonych pracowników.
b. Klucze do szafek pracowniczych są w posiadaniu Pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie i utrzymanie.
c. Klucze zapasowe są zabezpieczone przez firmę ochroniarską.
d. Pracownicy nie mogą używać dorabianych osobiście kluczy do pomieszczeń.
e. Osoby uprawnione do posiadania kluczy do pomieszczeń nie mogą ich udostępniać innym osobom i są zobowiązane do osobistego ich zwrotu w dniu pobrania, po zakończeniu pracy.
f. Osoby, które zagubiły klucz ponoszą odpowiedzialność materialną.

4. Bieżące postępowanie w trakcie dnia pracy

a. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
b. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
c. Po zakończeniu pracy, pracownicy są zobowiązani do:
   - ✓ wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych,
   - ✓ wyłączenia oświetlenia,
   - ✓ schowania dokumentów zawierających dane osobowe oraz pieczątek w szarkach z zamkiem
   - ✓ zabezpieczenia i zamknięcia okien i drzwi,
d. Za przestrzeganie w/w zasad bieżących odpowiadają kierownicy działów.

5. Sankcje

Naruszenie zasad polityki kluczy może spowodować wyciągnięcie następujących konsekwencji:

a. Poniesienie odpowiedzialności wynikających z Art. 52 kodeksu pracy,
b. Poniesienie odpowiedzialności wynikających z Art. 363 § 1 kodeksu cywilnego.

IV. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1. Wyposażenie informatyczne jest obsługiwane przez przeszkolony i upoważniony do tego personel.
2. Każdy element wyposażenia informatycznego jest jednoznacznie etykietowany, oznakowany lub zidentyfikowany w inny sposób.
3. Wyposażenie komputerowe stosowane w Zakładzie Mechanicznym „BUMAR-MIKULCZYCE" S.A jest przechowywane i eksploatowane w warunkach zapewniających jego prawidłowe funkcjonowanie, zgodnie z wytycznymi producentów.
4. Urządzenia poddaje się kontroli z częstotliwością wynikającą z ich rodzaju i wskazań wytwórców, zgodnie z opracowanym harmonogramem.
5. W Zakładzie stosowane jest tylko i wyłącznie oprogramowanie licencjonowane.
6. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane, w tym dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
7. Zabronione jest wykonywanie nieautoryzowanych kopii danych przetwarzanych przy użyciu systemów informatycznych.
8. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
9. Wszystkie komputery i laptopy działające w systemie informatycznym posiadają zainstalowane oprogramowanie antywirusowe, dodatkowo sprzęt posiadający połączenie z Internetem chroniony jest zaporą sieciową (firewall) programową lub sprzętową.
10. Użytkownicy laptopów zobowiązani są do:
    a. sporządzania regularnych (np. automatycznych) kopii bezpieczeństwa,
    b. przechowywania komputera przenośnego po zakończeniu pracy w warunkach zapewniających bezpieczeństwo,
    c. stosowania linki zabezpieczającej, w przypadku gdy laptop znajduje się bez nadzoru osoby upoważnionej w pomieszczeniu nie zamykanym na zamek.
11. Pomieszczenia, w których przechowywany jest sprzęt komputerowy i nośniki informacji są zabezpieczone przed dostępem osób postronnych.

V. Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe

Opis technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych.

1. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
2. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
3. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
4. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

5. Sprzęt komputerowy i nośniki przenośne w których przetwarza się dane osobowe i/ lub informacje prawnie chronione mają wdrożone środki ochrony kryptograficznej.

VI. Procedura - Dostęp podmiotów zewnętrznych

Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, w przypadku, gdy Administrator Danych powierza ich przetwarzanie firmom zewnętrznym.

1. Powierzenie przetwarzania danych podmiotom zewnętrznym następuje na podstawie umowy.
   - ✓ Umowa powierzenia przetwarzania danych – podpisywana z podmiotami, które przetwarzają dane osobowe „na zewnątrz" w formie outsourcingu. Przykładem takim jest Biuro Doskonalenia Kadr „ANDRAGOG" **-** świadczące szkolenia BHP.
2. Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A., korzysta wyłącznie z usług takich podmiotów przetwarzających dane osobowe, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. Wybrany pracownik prowadzi rejestr podmiotów zewnętrznych, którym Administrator udostępnia dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej.
4. Administrator Danych powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o umowę powierzenia przetwarzania danych. Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia przetwarzania danych osobowych. Podmiot zewnętrzny zobowiązany jest do stosowania zabezpieczeń określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 nr 100 poz. 1024).

VII. Procedura – Korzystanie z Internetu

Celem procedury jest określenie właściwego sposobu korzystania z sieci Internet, tak aby zachować bezpieczeństwo informacji.

1. W trakcie wykonywania czynności służbowych, użytkownicy tylko w przypadku uzasadnionej konieczności, (jeżeli ma to związek z ich aktualnie wykonywaną pracą) mogą uruchomić aplikację służącą do przeglądania stron internetowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Administratora Systemu i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez

prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

VIII. Procedura – Korzystanie z poczty elektronicznej

Celem procedury jest określenie właściwego sposobu przekazywania informacji, tak aby zachować bezpieczeństwo informacji przesyłanych zarówno wewnątrz Zakładu jak i poza (do podmiotów zewnętrznych).

1. Przekazywanie w treści maila danych osobowych jest zabronione. Dane osobowe muszą być przesyłane w szyfrowanych załącznikach. Hasło do zaszyfrowanego pliku wysyłamy inna drogą dystrybucji np. po przez wiadomość SMS.
2. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
3. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
4. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
5. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

IX. Procedura – Nadawanie uprawnień do przetwarzania danych osobowych

1. Procedura nadawania uprawnień do przetwarzania danych osobowych w Systemach informatycznych

a) Uprawnienia Użytkowników do przetwarzania danych osobowych w Systemach informatycznych Zakładu Mechanicznego ”BUMAR-MIKULCZYCE” S.A. są nadawane wyłącznie osobom posiadającym upoważnienia do przetwarzania danych osobowych wydane zgodnie z zasadami określonymi w Polityce Bezpieczeństwa Danych Osobowych.

b) Uprawnienia do Systemu Informatycznego służącego do przetwarzania danych osobowych są nadawane w zakresie zgodnym z upoważnieniem do przetwarzania danych osobowych wydanym osobie, której uprawnienia dotyczą. Zabronione jest nadawanie uprawnień w zakresie szerszym niż wynikający z wydanego upoważnienia do przetwarzania danych osobowych.

c) Tryb nadawania uprawnień do poszczególnych systemów służących do przetwarzania danych w Zakładzie jest uzależniony od rodzaju Systemu informatycznego:

- uprawnienia do Systemów informatycznych: ZUS Płatnik, KWZ: moduł Płace, ELINOR: moduł Kadry, ELINOR: moduł FK, UniRCP, SAMBA: Handel-CRM, SAMBA: Kadry-Absencje, Sekretariat, KWZ: moduł Umowy zlecenie i o dzieło są nadawane przez Administratora Systemu Informatycznego. Osoba wnioskująca o nadanie upoważnienia do przetwarzania danych osobowych,

po nadaniu niniejszego upoważnienia przez Administratora Danych Osobowych, informuje Administratora Systemu Informatycznego o zakresie nadanego upoważnienia. Administrator Systemu Informatycznego nadaje uprawnienia zgodnie z zakresem nadanego upoważnienia do przetwarzania danych osobowych i informuje o tym osobę wnioskującą o nadanie upoważnienia do przetwarzania danych osobowych i przekazuje nadany identyfikator Użytkownika celem odnotowania go w Ewidencji osób upoważnionych do przetwarzania danych osobowych.

d) Administrator Systemu Informatycznego ponosi odpowiedzialność służbową za przyznanie zbyt szerokiego zakresu uprawnień do przetwarzania danych osobowych w Systemie informatycznym w stosunku do zakresu upoważnienia do przetwarzania danych osobowych, nadanego przez Administratora Danych Osobowych.
e) W przypadku nadawania Użytkownikowi uprawnień po raz pierwszy, Administrator Systemu Informatycznego generuje identyfikator Użytkownika oraz hasło inicjujące.
f) Hasło inicjujące umożliwia pierwsze zalogowanie się Użytkownika do Systemu Informatycznego. Użytkownik jest zobowiązany niezwłocznie zmienić hasło inicjujące na hasło znane jedynie Użytkownikowi.
g) Identyfikator Użytkownika nie może być przydzielony powtórnie innej osobie.
h) Uprawnienia Użytkowników są nadawane w taki sposób, aby mieli oni możliwość logowania się do Systemów informatycznych z różnych stacji roboczych.
i) Kierownicy jednostek organizacyjnych odnotowują w Ewidencji osób upoważnionych fakt nadania uprawnień w Systemie informatycznym Użytkownikowi oraz identyfikator przypisany tej osobie.

2. Procedura zmiany uprawnień do przetwarzania danych osobowych w Systemach informatycznych

a) Zmiana uprawnień do przetwarzania danych osobowych w Systemie informatycznym jest dokonywana na podstawie zmienionego upoważnienia do przetwarzania danych osobowych i odbywa się zgodnie z procedurą zawartą w niniejszym Rozdziale.
b) Osoba wnioskująca o zmianę upoważnienia, po dokonaniu zmiany zakresu upoważnienia przez Administrującego Danych Osobowych informuje o zaistniałym fakcie Administratora Systemu Informatycznego.
c) Administrator Systemu Informatycznego dokonuje zmiany zakresu uprawnień do przetwarzania danych osobowych w Systemie informatycznym zgodnie ze zmianą zakresu upoważnienia do przetwarzania danych osobowych dokonaną przez Administratora Danych Osobowych. Zmiana zakresu uprawnień do przetwarzania danych osobowych w Systemie informatycznym następuje zgodnie z trybem określonym w punkcie 1.3 niniejszego Rozdziału.
d) Administrator Systemu Informatycznego, po dokonaniu zmiany zakresu uprawnień w Systemie Informatycznym, informuje drogą elektroniczną Osoba wnioskująca o zmianę upoważnienia o wprowadzonych modyfikacjach z zakresu uprawnień w Systemie informatycznym.
e) Kierownik danego działu odnotowują zmieniony zakres uprawnień w Systemie Informatycznym służącym do przetwarzania danych osobowych w Ewidencji osób upoważnionych do przetwarzania danych osobowych.

3. Odebranie uprawnień do przetwarzania danych osobowych w Systemach Informatycznych

a) Odebranie uprawnień do przetwarzania danych osobowych w Systemie informatycznym następuje niezwłocznie po ustaniu potrzeby posiadania uprawnień przez Użytkownika, w szczególności w przypadku odwołania upoważnienia do przetwarzania danych osobowych lub zmiany jego zakresu w taki sposób, iż nie jest niezbędny dalszy dostęp do określonego Systemu informatycznego.
b) Uprawnienia w Systemie informatycznym są odbierane przez Administratora Systemu Informatycznego.
c) Administrator Systemu Informatycznego informuje drogą elektroniczną kierownika danego działu o fakcie odebrania Użytkownikowi uprawnienia do przetwarzania danych osobowych w Systemie informatycznym.
d) Kierownik danego działu odnotowuje fakt odebrania uprawnienia do przetwarzania danych osobowych w Ewidencji osób upoważnionych do przetwarzania danych.

4. Zawieszenie uprawnień do przetwarzania danych osobowych w Systemach informatycznych

a) Uprawnienia Użytkownika mogą zostać zawieszone przez Administratora Systemu Informatycznego w przypadku, gdy bieżące działanie Użytkownika może spowodować zagrożenie dla bezpieczeństwa danych osobowych lub z powodu wystąpienia ogólnego zagrożenia bezpieczeństwa przetwarzania danych osobowych w Systemie informatycznym.
b) O zawieszeniu uprawnień Administrator Systemu Informatycznego informuje drogą elektroniczną Administratora Danych Osobowych.

5. Pozostałe postanowienia

a) W ramach prac administracyjnych Administrator Systemu Informatycznego prowadzi okresową kontrolę nieużywanych kont Użytkowników. W przypadku wykrycia takich kont i po wyjaśnieniu ich statusu Administratora Systemu Informatycznego dezaktywuje te konta.
b) Inspektor Ochrony Danych prowadzi nadzór nad procesem zarządzania uprawnieniami Użytkowników. Inspektor Ochrony Danych jest uprawniony do okresowego sprawdzania zakresu przysługujących Użytkownikom uprawnień w Systemie informatycznym z zakresem wydanego upoważnienia do przetwarzania danych osobowych oraz pod kątem zgodności z prowadzoną Ewidencją osób upoważnionych do przetwarzania danych osobowych. W przypadku stwierdzenia nieprawidłowości, Inspektor Ochrony Danych ma prawo wydawania poleceń mających na celu usunięcie uchybień oraz może wnioskować o wyciągnięcie konsekwencji służbowych wobec osób odpowiedzialnych za nieprawidłowe działania.

X. Metody i środki uwierzytelniania

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Ogólne zasady postępowania z hasłami

a. Pracownik po otrzymaniu od Administratora systemu w formie ustnej losowego hasła, loguje się za jego pomocą do systemu.
b. Po pierwszym logowaniu użytkownik zobowiązany jest do zmiany hasła.

c. Użytkownicy nie mogą używać tych samych identyfikatorów, wymieniać się nimi ani udostępniać konta komukolwiek innemu
d. Zabrania się udostępniania innym pracownikom hasła.
e. Zabrania się zapisywania hasła do programów przetwarzających dane osobowe.
f. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy, jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
g. Hasła, które muszą być zapisane w formie jawnej, zabezpiecza się w zalakowanej kopercie w szafie pancernej.

2. Hasła do sieci i serwera
a. Hasło musi składać się z co najmniej 8 znaków, musi zawierać małe i wielkie litery oraz cyfry i znak specjalny.
b. Hasła należy zmieniać regularnie, minimum co 6 miesięcy.

3. Hasła do programów przetwarzających dane osobowe
a. Hasło musi składać się z co najmniej 8 znaków, musi zawierać małe i wielkie litery oraz cyfry lub znak specjalny.
b. Hasła należy zmieniać regularnie, minimum co 30 dni.

4. Hasła administratora
a. Hasło musi składać się z co najmniej 8 znaków, musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
b. Hasło należy zmieniać regularnie, minimum co 30 dni.
c. Administrator zobowiązany jest do prowadzenia metryk haseł administratora, w tym hasła „root". Metryka hasła powinna zawierać: treść hasła, datę jego wprowadzenia do systemu, datę i powód awaryjnego udostępnienia hasła. Metryka powinna zostać zabezpieczona przed dostępem osób nieupoważnionych. Dostęp do metryki ma tylko i wyłącznie Administrator Danych Osobowych.
d. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

XI. Procedura - Rozpoczęcia, zawieszenia i zakończenia pracy

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Pracownik ma obowiązek utrzymywać ład i porządek na stanowisku pracy w godzinach jej wykonywania oraz po jej zakończeniu.
2. Na biurkach mogą znajdować się wyłącznie artykuły biurowe oraz inne dokumenty związane z wykonywaniem bieżących zadań.
3. Niedopuszczalne jest pozostawanie na biurku dokumentów, dokumentacji zawierającej dane osobowe oraz innych przedmiotów (m.in. książki, segregatory z dokumentami, pieczątki itd.) nie mających zastosowania z wykonywaną aktualnie pracą.
4. Pracownik spożywający posiłek przy stanowisku pracy zobowiązany jest zabezpieczyć dokumentację papierową oraz sprzęt komputerowy przed zniszczeniem.
5. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
6. Użytkownik jest zobowiązany do powiadomienia przełożonych o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.

7. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym Administratora systemu, który odpowiada za odblokowanie systemu użytkownikowi.
8. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wgląd do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu.
9. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest zamknąć dokumenty w szafach, zabezpieczyć inne dokumenty przed dostępem osób niepowołanych, zabezpieczyć dostęp do komputera - wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 5 minut system automatycznie aktywuje wygaszacz.
10. Niedopuszczalne są praktyki pozostawiania na stanowisku pracy samoprzylepnych kartek, luźno zapisanych notatek, kalendarzy lub innych dokumentów zawierających istotne informacje.
11. Wszelkie dokumenty papierowe zawierające istotne dane oraz dokumenty poddawane okresowej inwentaryzacji i zniszczeniu muszą być likwidowane przy użyciu niszczarki mechanicznej.
12. Niedopuszczalne jest wyrzucanie dokumentów zawierających istotne informacje do koszy na śmieci.
13. W przypadku wykonywania kopii dokumentu za pomocą ksero, skanera, faxu, należy sprawdzić czy wszystkie dokumenty zostały usunięte z urządzenia celem zminimalizowania przejęcia danego dokumentu przez osoby niepowołane.
14. Po zakończeniu pracy, użytkownik zobowiązany jest:
    - ✓ wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
    - ✓ zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe,
    - ✓ sprawdzić zamknięcie okien.

XII. Procedura – Tworzenie kopi zapasowych

Celem niniejszej procedury jest zapewnienie właściwego sposobu zabezpieczania danych zgromadzonych w systemie komputerowym poprzez wykonywanie ich kopii.

1. Kopie zapasowe wykonywane są na serwerze.
2. Kopie są wykonywane automatycznie zgodnie z przyjętym harmonogramem archiwizacji danych.
3. Harmonogram archiwizacji danych jest dostosowywany do ilości przechowywanych danych na komputerach/serwerach oraz ilości komputerów/serwerów.
4. Kopia systemu umieszczana jest na serwerze oraz na nośnikach zewnętrznych.
5. Administrator systemu dokonuje sprawdzania statusu wykonanych kopii bezpieczeństwa.
6. W przypadku wystąpienia problemu z kopią bezpieczeństwa Administrator systemu usuwa usterkę i kopia zostaje wykonana dnia następnego.

XIII. Procedura – Postępowanie z elektronicznymi nośnikami informacji i wydrukami

Celem niniejszej procedury jest zapewnienie właściwego sposobu zabezpieczania informacji zgromadzonych na nośnikach danych (płyta CD, płyta DVD, pendrive,

zewnętrzny dysk twardy), aby zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji na nich zapisanych.

1. **Przechowywanie kopii zapasowych**
   a) Kopie zapasowe przechowywane są w miejscu zabezpieczających je przed nieuprawnionym dostępem, przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
   b) Po zakończonym dniu pracy należy:
      - ✓ właściwie zabezpieczyć wykonane kopie zapasowe,
      - ✓ zamknąć pomieszczenie, w którym są one przechowywane.
   c) Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności zgodnie z procedurą - Postępowanie z nośnikami.
2. **Przekazanie i wynoszenie nośnika**
   a) W Zakładzie Mechanicznym „BUMAR-MIKULCZYCE" S.A nie wolno korzystać z prywatnych nośników.
   b) Nośniki służbowe wielokrotnego użytku (pendrive, zewnętrzny dysk twardy) należy opróżniać po każdym użyciu.
   c) Domyślnie nośniki nie opuszczają terenu Zakładu.
   d) Wyniesienie i powrót pamięci masowej poza teren Zakładu należy ewidencjonować.
   e) W przypadku konieczności przekazania podmiotowi nieuprawnionemu nośnika danych należy pozbawić wcześniej nośnik wszelkich zapisów danych wrażliwych, w tym danych osobowych, w sposób uniemożliwiający ich odzyskanie, np. poprzez sformatowanie nośnika przy zastosowaniu odpowiedniego oprogramowania.
   f) W przypadku konieczności naprawy nośnika (gdy naprawa jest możliwa), należy usunąć z nośnika dane, w tym dane osobowe w sposób uniemożliwiający ich odzyskanie albo dokonać naprawy nośnika pod nadzorem osoby upoważnionej.
3. **Przechowywanie danych na nośnikach zewnętrznych**
   a) W okresie przechowywania należy kontrolować stan nośnika oraz danych na nim umieszczonych, w tym kopii zapasowych, gdyż w trakcie przechowywania nośniki tracą żywotność, a co za tym idzie dane na nich zapisane mogą fizycznie zniknąć z nośnika.
   b) W przypadku stwierdzenia uszkodzenia (np. rysy na powierzchni płyty), pogorszenia jakości przechowywanych danych (np. problemy z odczytem, niekompletny odczyt) czy też upływ czasu koniecznym jest wykonanie kopii danych na inny (nowy) nośnik, natomiast stary należy zutylizować.
   c) Nośniki zawierające dane, w tym dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.
   d) W Zakładzie Mechanicznym „BUMAR – MIKULCZYCE" S.A obowiązuje absolutny zakaz użytkowania prywatnych zewnętrznych nośników danych, za wyjątkiem sytuacji, w której zgodę wyraził informatyk**.**
4. **Zabezpieczenie dokumentów i wydruków**
   a) Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
   b) Pracownicy są zobowiązani do zabezpieczania dokumentów (np. zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych po zakończeniu pracy (tzw. Polityka czystego biurka).
   c) Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach bez nadzoru.
   d) Pracownicy są zobowiązani do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

e) Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są wszyscy pracownicy.

5. Likwidacja / Wycofanie nośnika – pendrive, dysk twardy

a) Niszczenie nośników dokonuje się w następujący sposób:
   - Dyski twarde z komputerów i serwerów komisyjnie uszkadza się poprzez mocne uderzenie ciężkim tępym narzędziem, aż do fizycznego ich zniszczenia, lub poprzez wyspecjalizowaną firmę w procesie demagnetyzacji.
   - Płyty CD-R, CD-RW, DVD, DVD-RW, BR, BR-RW oraz karty pamięci przełamuje się na kilka części, lub niszczy w niszczarce przeznaczonej do utylizacji płyt CD.
   - Taśmy magnetyczne wyciąga się z obudowy i przecina na wiele części.
   - Pamięci flash jak i dyski przenośne uszkadza się w podobny sposób jak dyski twarde poprzez demagnetyzację lub zniszczenie do fizycznego rozpadu.

b) Z dysków przeznaczonych do likwidacji Administrator systemu zobowiązany jest zniszczyć go komisyjnie oraz sporządzić protokół jego zniszczenia.

c) Administrator systemu zniszczone w ten sposób nośniki zobowiązany jest przekazać firmie zajmującej się utylizacją odpadów elektronicznych.

d) Administrator systemu zobowiązany jest do zarejestrowania karty przekazania odpadu elektronicznego otrzymanej od firmy utylizacyjnej.

XIV. Procedura - Zabezpieczenie systemu informatycznego, w tym przed wirusami komputerowymi

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

1. Ochrona antywirusowa

a. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada Administrator Systemu, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
b. System antywirusowy zainstalowano na serwerze oraz na wszystkich komputerach i laptopach działających w systemie informatycznym.
c. System antywirusowy zapewnia ochronę systemu operacyjnego, przechowywanych plików oraz poczty wychodzącej i przychodzącej.
d. Użytkownicy zobowiązani są do skanowania plików skanerem antywirusowym.
e. Administrator Systemu oraz użytkownicy zapewniają stałą aktywność programu antywirusowego. Tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
f. Aktualizacja definicji wirusów odbywa się automatycznie przez system.
g. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić Administratora Systemu.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

a. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada Administrator Systemu.
b. Stosowana jest zapora sieciowa (firewall) sprzętowa lub programowa.
c. Sieć bezprzewodową zabezpieczono protokołem WPA2.

XV. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   - ✓ osoby, której dane dotyczą,
   - ✓ osoby, upoważnionej do przetwarzania danych,
   - ✓ podmiotu, któremu powierzono przetwarzanie danych,
   - ✓ organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
2. System przetwarzający dane osobowe udostępniane odbiorcom musi umożliwiać rejestrację:
   - ✓ nazwy jednostki organizacyjnej lub imienia i nazwiska osoby, której udostępniono dane,
   - ✓ zakresu udostępnianych danych,
   - ✓ daty udostępnienia.
3. Dane osobowe przetwarzane przez Zakład Mechaniczny „BUMAR-MIKULCZYCE" S.A. udostępnia się Odbiorcy danych w formie kopii na pisemny wniosek ze wskazaniem przez Odbiorcę podstawy prawnej legalizującej przetwarzanie danych osobowych.
4. Zgody na udostępnienie danych udziela Prezes Zarządu.
5. Odnotowanie informacji o udostępnieniu danych (komu, zakres, data) następuje niezwłocznie po udostępnieniu tych danych w systemie informatycznym.
6. Administrator Danych Osobowych odpowiada za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem.
7. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub wyciągu z rejestru papierowego, a raport przekazywany jest tej osobie.

XVI. Procedura – Administrowanie i monitoring systemów informatycznych (przeglądy i konserwacja)

Celem procedury jest pisemne określenie przebiegu postępowania w celu zapewnienia ciągłości pracy urządzeń informatycznych, integralności systemów oraz ochrony informacji, w tym danych osobowych zawartych w systemach.

1. Ogólne

a. Za ciągłe monitorowanie działania systemów informatycznych, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email, itd., odpowiedzialny jest Administrator systemu, który na bieżąco analizuje stopień spełnienia wymagań dotyczących ochrony danych.
b. Administrator systemu dokonuje wszelkich czynności związanych z nadaniem, modyfikacją oraz usunięciem uprawnień użytkowników zgodnie z procedurą – Kontrola dostępu.
c. Administrator systemu obserwuje zachowania pracowników i identyfikuje te stwarzające zagrożenia. Zwraca uwagę takim pracownikom lub przełożony odbiera uprawnienia pracownikowi.
d. Administrator systemu podejmuje natychmiastową reakcję na powiadomienia o braku prądu.
e. Administrator systemu podejmuje natychmiastową reakcję na sygnały krytyczne w systemie i podejmuje działania w celu usunięcia incydentów.

2. **Oprogramowanie**
   a. Administrator systemu instaluje/konfiguruje/zarządza systemami operacyjnymi do których został upoważniony.
   b. W przypadku konieczności zainstalowania nowego oprogramowania, Pracownik przekazuje zatwierdzone przez przełożonego (w formie ustnej lub pisemnej) zapotrzebowanie Administratorowi systemu, który analizuje, czy wymagana funkcjonalność nie jest już dostępna. Następnie jeśli nie, wyszukuje narzędzia ją zapewniające i sprawdza, czy dane oprogramowanie może kolidować z innym, już dostępnym. Po doborze oprogramowania, korzystając z nośnika danych instaluje na wyznaczonej maszynie oprogramowanie. Jego legalność w razie potrzeby potwierdza kluczem, kodem, itp.
   c. W przypadku pojawienia się aktualizacji oprogramowania, Administrator systemu sprawdza zakres aktualizacji oraz czy nie spowoduje ona problemów we współpracy z innymi programami, a następnie dokonuje aktualizacji systemów operacyjnych oraz usług do najnowszych stabilnych wersji oprogramowania. Jego legalność w razie potrzeby potwierdza kluczem, kodem, itp.
   d. W przypadku wykrycia lub otrzymania informacji o zbędnym oprogramowaniu, Administrator systemu po uprzednim dokonaniu analizy zapotrzebowania na dane oprogramowanie usuwa je z wyznaczonej maszyny.
3. **Sieć**
   a. Administrator systemu analizuje na bieżąco zapotrzebowanie istniejących stanowisk jak również planowanych oraz całego Zakładu na dostęp do sieci.
   b. Administrator systemu dokonuje doboru sprzętu sieciowego oraz projektuje okablowanie strukturalne budynku i wszystkich pomieszczeń tak, aby spełniało wymagania poszczególnych stanowisk oraz całego Zakładu.
   c. Administrator systemu przygotowuje konfigurację całego sprzętu przy okazji planowania okablowania strukturalnego oraz odpowiednią konfigurację sprzętu.
   d. Jeśli tego wymaga sytuacja, Administrator systemu na podstawie zgłaszanych problemów, a także monitorowania sprzętu i dziennika systemowego wybiera i wprowadza nową konfigurację sieci oraz aktualizuje sprzęt sieciowy dostosowując do niego konfigurację.
4. **Sprzęt**
   a. Administrator systemu analizuje zgłoszenia użytkowników i planowane zapotrzebowanie na nowy sprzęt.
   b. Administrator systemu sprawdza bieżący stan sprzętu w Zakładzie i na tej podstawie przygotowuje listy urządzeń do aktualizacji/utylizacji/rekonfiguracji.
   c. Administrator systemu wymienia stare części na nowe oraz stary sprzęt na nowy.
5. **Konserwacja systemu**
   a. Przegląd i konserwacja systemu informatycznego wykonywane są w terminach określonych przez producentów systemu lub zgodnie z harmonogramem, jednak nie rzadziej, niż raz w roku.
   b. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada Administrator systemu.
   c. Administrator systemu sprawdza wszelkie ostrzeżenia generowane przez system.
   d. W razie potrzeby Administrator systemu dokonuje zmiany w konfiguracji systemu.

XVII. Procedura – Reakcja na naruszenia związane z bezpieczeństwem danych osobowych

Naruszeniami bezpieczeństwa danych osobowych są:

1. Przypadki naruszenia poufności (ujawnienie niepowołanym osobom), integralności (uszkodzenie, przekłamanie, zniszczenie) i dostępności (dane nie są dostępne w użytecznej postaci na żądanie uprawnionych użytkowników) danych, niezależnie od ich nośnika, w tym także przechowywanych i przetwarzanych w systemach informatycznych oraz transmitowanych przez łącza sieci.
2. Niedostępność oraz działania niezgodne ze specyfikacją (błędny) systemów informatycznych, zwłaszcza systemów i aplikacji krytycznych, z wyłączeniem kontrolowanych i zaplanowanych prac oraz dysfunkcji niemających wpływu na bezpieczeństwo informacji.
3. Infekcje, propagacja i działanie szkodliwego oprogramowania (malware, wirus, robak internetowy, koń trojański, spyware, itp.).
4. Niewłaściwe wykorzystywanie lub nadużywanie zasobów informacyjnych.
5. Ataki nieautoryzowanego dostępu do aplikacji, systemów oraz ataki eskalacji poziomu uprawnień w systemach.
6. Kradzież lub zniszczenie urządzeń przetwarzających lub/i przechowujących informacje oraz nośników danych.
7. Ataki socjotechniczne, ataki z wykorzystaniem phishing'u, skimming'u oraz innych technik zagrażających naruszeniu poufności, dostępności i integralności informacji.
8. Łamanie zasad regulacji wewnętrznych obowiązujących w Zakładzie w obszarze bezpieczeństwa ochrony danych lub wynikających z nich zapisów w umowach z Podmiotami Zewnętrznymi oraz przepisów prawa powszechnego regulujących kwestie bezpieczeństwa w działalności Zakładu (w tym rozporządzeń UE).

Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

1. Pracownik podejrzewający, że zaistniało zdarzenie, które powinno być zaklasyfikowane jako naruszenie bezpieczeństwa zgłasza jak najszybciej dane zdarzenie do Inspektora Ochrony Danych.
2. Naruszenia zgłaszane są w formie pisemnej, telefonicznej lub przy pomocy poczty elektronicznej.
3. Inspektor Ochrony Danych ocenia skalę zdarzenia.

Weryfikacja naruszeń bezpieczeństwa danych osobowych

1. Inspektor Ochrony Danych rejestruje wszystkie zgłoszenia naruszeń w „Rejestrze naruszeń", a następnie weryfikuje zgłoszenie na podstawie przewidywanych następstw.
2. Analizuje prawdopodobieństwo, czy naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych.

Zamknięcie zdarzenia niebędącego naruszeniem bezpieczeństwa danych osobowych

1. W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako naruszenie bezpieczeństwa ochrony danych Inspektor Ochrony Danych informuje pracownika zgłaszającego zdarzenie wyjaśniając mu zasadność podjętej decyzji, a następnie zamyka dane zgłoszenie.
2. W wybranych przypadkach Inspektor Ochrony Danych decyduje o publikacji informacji o kwalifikacji danego zdarzenia do wszystkich interesariuszy (np. poprzez wywieszenie informacji na tablicy ogłoszeń lub rozesłanie maili do stron zainteresowanych).

Obsługa naruszenia

1. Inspektor Ochrony Danych informuje o wystąpieniu naruszenia bezpieczeństwa ochrony danych osoby związane z naruszeniem.

2. Inspektor Ochrony Danych rejestruje naruszenie w „Rejestrze naruszeń" oraz powiadamia wybranego pracownika.
3. Inspektor Ochrony Danych i/lub wybrany pracownik podejmuje działania minimalizujące skutki wystąpienia naruszenia. Gromadzi materiał dowodowy (np. logi systemowe, zabezpiecza miejsce włamania, dokonuje zabezpieczenia plików elektronicznych itp.).
4. Inspektor Ochrony Danych i/lub wybrany pracownik podejmuje działania niezbędne do usunięcia skutków zgłoszonego naruszenia bezpieczeństwa.
5. W przypadku potrzeby zachowania materiału dowodowego naruszenia w systemach informatycznych Prezes Zarządu ściśle współpracuje z Administratorem systemów w zakresie zachowania pełnej integralności i niezaprzeczalności dowodu.

Zgłaszanie naruszeń danych osobowych

1. W sytuacji gdy naruszenie bezpieczeństwa danych osobowych wiąże się z udostępnieniem danych osobowych nie upoważnionej osobie (m.in. wypłynięcie danych), należy przeanalizować skalę naruszenia, oraz czy takie naruszenie będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. W sytuacji gdy istnieje takie ryzyko, naruszenie należy zgłosić do Urzędu Ochrony Danych Osobowych (na stronie https://uodo.gov.pl/pl/134/233) oraz do osób których dane osobowe zostały udostępnione.
3. Zgłoszenie do UODO musi:
   a) opisywać charakter naruszenia ochrony danych osobowych;
   b) zawierać imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zakończenie obsługi naruszenia

1. Po zakończeniu obsługi zgłoszenia Inspektor Ochrony Danych uzupełnia „Rejestr naruszeń".

Działania kontrolne i korygujące

1. Inspektor Ochrony Danych oraz Administrator systemów regularnie przeglądają naruszenia bezpieczeństwa danych osobowych uwzględniając:
   - ich częstotliwość,
   - obszar występowania,
   - powtarzalność naruszeń,
   - skuteczność działań korygujących i minimalizujących ponowne wystąpienie.
2. Inspektor Ochrony Danych przygotowuje Raport z przeglądu naruszeń bezpieczeństwa danych osobowych na podstawie Rejestru naruszeń - F/IZSI/6.

XVIII. - Postanowienia końcowe

1. Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody Prezesa Zarządu.

2. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszej Instrukcji.
3. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
4. Zmiana dokonana w załączniku do niniejszej Instrukcji powoduje aktualizację danego załącznika, nie powoduje natomiast zmiany całości dokumentu. Po dokonaniu aktualizacji załącznika jego wcześniejsza wersja automatycznie traci ważność.