administracyjnym.

3. W przypadku zmian w przepisach prawa lub nałożenia na Jednostkę przez naczelne lub centralne organy administracji państwowej obowiązku wykonania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej, w związku z realizacją których występuje konieczność przetwarzania danych osobowych, pracownicy uzyskujący taką informację zobowiązani są do poinformowania przełożonego, który we współpracy z IOD, na podstawie przekazanych informacji dokonuje uzupełnienia lub zmian w Rejestrze czynności przetwarzania danych osobowych.
4. W przypadku uzyskania informacji przez pracownika Jednostki o powierzeniu przetwarzania danych osobowych Jednostce – na podstawie umowy lub innego instrumentu prawnego – pracownik ten jest zobowiązany do poinformowania przełożonego, który we współpracy z IOD, na podstawie przekazanych informacji dokonuje uzupełnienia lub zmian w Rejestrze wszystkich kategorii czynności przetwarzania
5. Rejestry, o których mowa w ust. 1 i 2 przyjmują formę pisemną, jak również formę elektroniczną, która powinna być prowadzona w systemie informatycznym równolegle z formę pisemną.
6. Administrator jest zobowiązany do udostępnienia ww. rejestrów na żądanie organu nadzorczego. Ww. rejestry nie stanowią dokumentów udostępnianych na podstawie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2022 r., poz. 902).
7. IOD we współpracy z Administratorem, przygotowuje i aktualizuje rejestry, o których mowa w ust. 1 i 2.

Objaśnienie:

Rejestr czynności przetwarzania danych osobowych prowadzony jest przez Jednostkę w przypadku, w którym Jednostka występuje jako Administrator danych osobowych.

W Rejestrze tym zamieszcza się następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela Administratora oraz Inspektora ochrony danych,
b) cele przetwarzania,
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Rejestr wszystkich kategorii czynności przetwarzania prowadzony jest przez Jednostkę, w przypadku, w którym Jednostka występuje jako Podmiot przetwarzający dane osobowe na zlecenie.

W Rejestrze tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe Podmiotu przetwarzającego lub Podmiotów przetwarzających oraz każdego Administratora, w imieniu którego działa Podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela Administratora lub Podmiotu przetwarzającego oraz Inspektora ochrony danych,
b) kategorie przetwarzań dokonywanych w imieniu każdego z Administratorów,
c) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Art. 12. Szkolenia z zakresu ochrony danych osobowych

1. Każda osoba, która uzyskuje upoważnienie do przetwarzania danych osobowych ma obowiązek zapoznać się z najważniejszymi informacjami o obowiązkach związanych z przetwarzaniem danych osobowych. Wzór informatora zawierającego ww. informacje stanowi **załącznik nr 9** do Polityki.
2. IOD lub inna wyznaczona osoba, z własnej inicjatywy lub na wniosek Administratora, przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych dla osób je przetwarzających.
3. Dodatkowo szkolenia wewnętrzne są przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ochrony danych osobowych, odpowiednio uwzględniając postanowienie ust. 2.
4. Każde szkolenie wewnętrzne powinno być udokumentowane poprzez sporządzenie dokumentów potwierdzających uczestnictwo w takim szkoleniu przez jego uczestników (lista obecności lub zaświadczenie/certyfikat imienny dla Użytkownika).

Art. 13. Dostęp do danych osobowych przez podmioty trzecie

1. Administrator może przekazać podmiotowi trzeciemu (niebędącemu osobą, której dane dotyczą) przetwarzane przez siebie dane osobowe w ramach:
   1) udostępnienia - jeżeli jest to przewidziane w powszechnie obowiązujących przepisach prawa;
   2) powierzenia - jeżeli podmiot trzeci przetwarza dane w imieniu Administratora i na jego udokumentowane polecenie w rozumieniu art. 28 RODO.
2. W przypadku powierzenia przetwarzania danych konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem

a Podmiotem przetwarzającym dane na zlecenie, który przetwarza dane w imieniu Administratora (zwanym również Procesorem) bądź posłużenie się innym instrumentem prawnym, który podlega prawu Unii lub prawu polskiemu i wiąże zarówno Podmiot przetwarzający jak i Administratora.

3. Administrator przed powierzeniem przetwarzania danych osobowych zobligowany jest do uzyskania informacji o stosowanych przez Procesora środkach technicznych i organizacyjnych, za pomocą listy kontrolnej procesora stanowiącej **załącznik nr 10** do Polityki.
4. IOD przygotowuje (we współpracy z osobami upoważnionymi, a także osobą reprezentującą Administratora) i weryfikuje umowy powierzenia przetwarzania danych lub inne instrumenty prawne przed ich zawarciem.
5. Administrator przyjął minimalne wymagania co do treści umowy powierzenia przetwarzania danych, której wzór stanowi **załącznik nr 11** do Polityki.
6. Administrator po zawarciu każdej umowy powierzenia – za pośrednictwem wyznaczonego pracownika – odnotowuje ten fakt w rejestrze zawartych umów powierzenia, którego wzór stanowi **załącznik nr 12** do Polityki.

Art. 14. Sposób weryfikacji Podmiotu Przetwarzającego (Procesora)

1. W przypadku powierzenia przetwarzania danych konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem a Podmiotem przetwarzającym dane na zlecenie, który przetwarza dane w imieniu Administratora (zwanym również Procesorem) bądź posłużenie się innym instrumentem prawnym, który podlega prawu Unii lub prawu polskiemu i wiąże zarówno Podmiot przetwarzający jak i Administratora.
2. Administrator przed powierzeniem przetwarzania danych osobowych zobligowany jest do uzyskania informacji o stosowanych przez podmiot, któremu zamierza powierzyć dane osobowe środkach technicznych i organizacyjnych, za pomocą listy kontrolnej stanowiącej **załącznik nr 10** do Polityki. Lista kontrolna powinna zostać przekazana

potencjalnemu Podmiotowi przetwarzającemu na etapie negocjowania umowy na świadczenie usług.

3. W przypadku wątpliwości w zakresie udzielonych przez potencjalny Podmiot przetwarzający informacji w liście kontrolnej, Jednostka powinna dokonać konsultacji z IOD czy ww. podmiot zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych by przetwarzanie spełniało wymogi rozporządzenia RODO i chroniło prawa osób, których dane dotyczą.
4. IOD przygotowuje (we współpracy z osobami upoważnionymi, a także osobą reprezentującą Administratora) i weryfikuje umowy powierzenia przetwarzania danych lub inne instrumenty prawne przed ich zawarciem.
5. Administrator przyjął minimalne wymagania co do treści umowy powierzenia przetwarzania danych, której wzór stanowi **załącznik nr 11** do Polityki.
6. W przypadku kiedy odpowiedzi udzielone przez Podmiot przetwarzający wskazują iż nie ma od wdrożonych żadnych środków technicznych, administrator decydując się na powierzenie przetwarzania danych określa minimalne zabezpieczenia które musi wdrożyć podmiot przetwarzający, w umowie powierzenia przetwarzania danych osobowych.

Art. 15. Jednostka w roli Podmiotu przetwarzającego (Procesora)

1. Jednostka, w związku z powierzeniem przetwarzania danych osobowych przez inny podmiot (odrębnego Administratora) występuje w roli Podmiotu przetwarzającego (Procesora), o którym mowa w art. 4 pkt 8 RODO.
2. Powierzenie zadań przez inny podmiot powinno nastąpić na mocy zawartej umowy powierzenia danych, o której mowa w art. 28 ust. 3 RODO lub innego instrumentu prawego.
3. Jednostka występująca w roli Podmiotu przetwarzającego (Procesora) zobowiązana jest stosować środki techniczne i organizacyjne aby zapewnić powierzonym danym należytą ochronę zgodnie z art. 24 i 32 RODO.

4. Szczegółowe obowiązki dotyczące ochrony danych osobowych powinna regulować umowa powierzenia przetwarzania danych, o której mowa w pkt 2 niniejszego artykułu.

Art. 16. Zasady anonimizacji danych osobowych

1. Osoba sporządzająca dokumenty przeznaczone do udostępnienia w Biuletynie Informacji Publicznej Jednostki jest zobowiązana do ich oceny pod względem dopuszczalności publikacji danych osobowych osób fizycznych niepełniących funkcji publicznych lub kierowniczych.
2. Osoba sporządzająca dokumenty przeznaczone do udostępnienia w Biuletynie Informacji Publicznej Jednostki jest zobowiązana do dokonania analizy legalności publikacji danych osobowych zawartych w dokumentach oraz w razie konieczności do dokonania ich anonimizacji.
3. Na podstawie obowiązujących przepisów o dostępie do informacji publicznej zaleca się stosowanie następujących zasad anonimizacji danych, z uwzględnieniem wyjątków wynikających z przepisów prawa:
   1) w przypadku udostępniania informacji o osobie fizycznej anonimizacji – co do zasady – podlegają:
      a) imię i nazwisko, chyba że dane te są zawarte w umowach podlegających publikacji w Biuletynie Informacji Publicznej,
      b) numer PESEL oraz NIP,
      c) data i miejsce urodzenia,
      d) numer dokumentu, za pomocą którego można zidentyfikować osobę fizyczną (np. dowód, paszport, prawo jazdy, legitymacja, koncesja itp.),
      e) adres zamieszkania, zameldowania lub pobytu,
      f) numer telefonu lub faksu,
      g) adres e-mail,
      h) numer rachunku bankowego,
      i) numer działki i obręb,
      j) numer księgi wieczystej,

k) informacje o zobowiązaniach finansowych (chyba że dane te podlegają publikacji w Biuletynie Informacji Publicznej),

l) informacje o stanie zdrowia, sytuacji finansowej, społecznej itp.,

m) inne dane pozwalające zidentyfikować osobę fizyczną lub naruszyć jej prawa i wolności;

2) w przypadku udostępniania wyciągów z rachunków bankowych lub dokumentacji księgowej (w tym faktur) anonimizacji podlegają:

a) imię i nazwisko (chyba że dane te są zawarte w umowach podlegających publikacji w Biuletynie Informacji Publicznej),

b) numer PESEL oraz NIP,

c) adres zamieszkania, zameldowania lub pobytu,

d) numer rachunku bankowego;

3) anonimizacji nie podlega natomiast imię i nazwisko usługodawcy lub nazwa firmy realizującej usługę, informacja o wykonanej usłudze oraz kwota, za jaką usługa została wykonana;

4) w przypadku udostępniania kopii innych dokumentów Jednostki dodatkowo anonimizacji podlegają wszystkie informacje, które mogą bezpośrednio zidentyfikować osobę fizyczną lub inne osoby fizyczne biorące udział w realizacji spraw.

4. Opisane wyżej zasady anonimizacji należy traktować jako reguły ogólne anonimizacji, które powinny być każdorazowo indywidualnie weryfikowane w przypadku udostępniania danych.

5. Anonimizacji nie podlegają w żadnym przypadku:

1) nazwy organów, urzędów oraz instytucji publicznych;

2) nazwy organizacji międzynarodowych;

3) nazwy sądów;

4) nazwy spółek Skarbu Państwa;

5) dane osób reprezentujących Administratora;

6) dane pracowników Administratora w zakresie realizacji zadań określonych

w regulaminie Jednostki;

7) dane członków zespołów, komisji, rad i innych powołanych do realizacji zadań;
8) nazwy dokumentów np. uchwała, zarządzenie, umowa, porozumienie, aneks, a także elementy dokumentów, które nie naruszają praw i wolności osoby;
9) imiona i nazwiska autorów cytowanych książek, komentarzy, artykułów naukowych, jeśli ich prace były wykorzystywane w treści dokumentów urzędowych podlegających udostępnieniu;
10) oznaczenie czasu tj. informacje o latach, miesiącach, dniach, godzinach, przedziałach czasowych, jak też daty wytworzenia dokumentów, z wyjątkiem daty urodzenia osoby fizycznej;
11) dane, co do których wyrażona jest pisemna zgoda na ich ujawnienie w Biuletynie Informacji Publicznej (np. petycje).

Art. 17. Procedura przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej

1. Administrator udostępnia publicznie dane osobowe w Biuletynie Informacji Publicznej zgodnie z zasadami określonymi w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2022 r. poz. 902) i innych przepisach prawa powszechnie obowiązującego.
2. Administrator, z uwzględnieniem zasady ograniczenia przechowywania zapewnia, że przechowuje dane osobowe publikowane w Biuletynie Informacji Publicznej w formie umożliwiającej identyfikację podmiotu danych przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane (okres retencji).
3. W przypadkach, gdy okres retencji danych osobowych publikowanych w Biuletynie Informacji Publicznej nie wynika wyraźnie z przepisów prawa, Administrator ustala niniejsze okresy samodzielnie, uwzględniając ogólne zasady przetwarzania danych osobowych przewidziane w RODO, w tym przede wszystkim zasadę ograniczenia

przechowywania określoną w art. 5 ust. 1 lit. e. Wszystkie ustalone okresy retencji zostają uwzględnione w treści Rejestru czynności przetwarzania danych osobowych prowadzonego przez Administratora, zwanego dalej Rejestrem.

4. Dane osobowe mogą być przetwarzane dłużej niż wynosi okres retencji w przypadku, gdy są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (na zasadach określonych w art. 89 ust. 1 RODO) pod warunkiem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności podmiotów danych.
5. Administrator – za pośrednictwem wyznaczonego pracownika cyklicznie tj. nie rzadziej niż 1 raz w roku posiada obowiązek dokonania przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej. Poza okresowymi przeglądami Administrator przeprowadza również przeglądy ww. danych, jeśli zajdzie przynajmniej jedna z poniższych sytuacji:
   1) zmienione zostaną powszechnie obowiązujące przepisy prawa mające wpływ na okres retencji;
   2) organ nadzorczy lub organ kontrolujący wydadzą zalecenia dotyczące przeglądu danych;
   3) zostanie wydana uzasadniona decyzja Administratora, o której zostaną poinformowane osoby zatrudnione w organizacji Administratora oraz z nią współpracujące.
6. Wszelkie przeglądy danych osobowych publikowanych w Biuletynie Informacji Publicznej podlegają udokumentowaniu w postaci stosownego dokumentu i są przechowywane w biurze Jednostki.

Art. 18. Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe

1. W stosunku do dokumentów papierowych stanowiących wydruki z systemu

informatycznego Jednostki oraz wszelkich innych dokumentów zawierających dane osobowe, osoby upoważnione są zobowiązane do zachowania następujących środków ostrożności:

1) wydruki z systemu informatycznego i wszelkie inne dokumenty zawierające dane osobowe powinny być niedostępne dla osób nieuprawnionych;
2) wydruki z systemu informatycznego i wszelkie inne dokumenty zawierające dane osobowe nie mogą być pozostawione w drukarce lub kserokopiarce ogólnodostępnej;
3) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki właściwej klasy;
4) dokumenty zawierające dane osobowe, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

Art. 19. Naruszenia ochrony danych osobowych

1. Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych.
2. Procedura zarządzania naruszeniami ochrony danych stanowi **załącznik nr 13** do Polityki.

Rozdział III
Procedury zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Art. 20. Zasady zarządzania uprawnieniami Użytkowników w systemach

informatycznych

1. Obsługa informatyczna na ustną dyspozycję Administratora tworzy konta dostępu do systemów informatycznych.
2. Obsługa informatyczna dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień Użytkowników systemów informatycznych na podstawie ustnej dyspozycji skierowanej od Administratora.
3. W przypadku zmiany uprawnień do systemów informatycznych Administratora wydaje nowe upoważnienie do przetwarzania danych osobowych.

Art. 21. Zasady zabezpieczenia dostępu do systemów informatycznych

1. W przypadku dostępu Użytkowników do systemów informatycznych (dziedzinowych i operacyjnych) należy stosować metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora/login-u oraz hasła.
2. Hasło powinno składać się z unikalnego zestawu znaków, zawierających małe i wielkie litery, cyfry oraz znaki specjalne. Hasło powinno być regularnie zmieniane przez Użytkownika oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej. Hasło co do zasady powinno się składać z minimum 12 znaków i być zmieniane co min. 180 dni. Hasła do systemów dziedzinowych powinny być tworzone w schemacie określonym przez dostawcę oprogramowania.
3. Użytkownik zobowiązany jest do zachowania poufności hasła i niezapisywania go w sposób jawny.
4. Hasła administracyjne do urządzeń i systemów informatycznych, w tym baz danych, winny być przechowywane w zapieczętowanej kopercie w miejscu wskazanym przez Administratora.

Art. 22. Zasady zarządzania sprzętem elektronicznym i oprogramowaniem

1. Użytkownik zobowiązany jest korzystać ze sprzętu elektronicznego w sposób zgodny

z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.

2. Użytkownik ma obowiązek niezwłocznie zgłosić Administratorowi utratę lub zniszczenie powierzonego sprzętu.
3. Użytkownik nie może bez zgody Administratora instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać do systemu informatycznego niezatwierdzonych urządzeń.
4. Użytkownik nie może bez zgody Administratora korzystać z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive'y) do wykonywania zadań służbowych. Szczegółowa procedura użytkowania prywatnych urządzeń elektronicznych przy pracy zdalnej stanowi **załącznik nr 14** do Polityki.
5. Administrator ma prawo do monitorowania sprzętu służbowego wykorzystywanego przez Użytkowników. O fakcie monitorowania Administrator zobowiązany jest powiadomić Użytkowników, zgodnie z przepisami Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2023 r. poz. 1465) nie później niż 2 tygodnie przed jego uruchomieniem.
6. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w Jednostce.

Art. 23. Zasady wykonywania kopii bezpieczeństwa

1. W celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania Jednostki tworzy się kopie zapasowe danych.
2. Kopią zapasową objęte są: dane istotne dla funkcjonowania Jednostki, systemy informatyczne o ile takie są w jednostce wdrożone.
3. Kopie zapasowe nie powinny znajdować się w tym samym pomieszczeniu co dane źródłowe.

4. Za sporządzenie kopii zapasowych odpowiedzialny jest pracownik wyznaczony przez Administratora.
5. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych dokumentów znajdujących się na lokalnych dyskach twardych.
6. Obsługa informatyczna Jednostki zobowiązana jest do testowania kopii zapasowych, w tym celu powinna:
   1) uruchomić środowisko testowe do testowania kopii zapasowej;
   2) rozpocząć proces symulacji przywracania kopii zapasowej;
   3) zweryfikować poprawność przywróconych danych;
   4) zakończyć sprawdzanie poprawności wykonanej kopii zapasowej;
   5) usunąć dane ze środowiska testowego.

Art. 24. Zasady korzystania z poczty elektronicznej

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu poczty elektronicznej wyłącznie w celu prowadzenia korespondencji służbowej.
2. Użytkownik nie może używać służbowego adresu poczty elektronicznej do celów prywatnych, w szczególności do rejestracji w serwisach społecznościowych, dokonywania zakupów w sklepach internetowych itp.
3. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu poczty elektronicznej odbiorcy wiadomości.
4. Użytkownik podczas wysyłania wiadomości e-mail do wielu adresatów jednocześnie, powinien użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie wiadomości e-mail do wielu adresatów z użyciem opcji „Do wiadomości - DW".
5. Użytkownik powinien zastosować zabezpieczenia kryptograficzne przy przesyłaniu załączników do wiadomości e-mail. Zabezpieczenia kryptograficzne mogą polegać na przesłaniu zahasłowanych plików w formie załącznika, jednak hasło powinno być przekazane adresatowi za pośrednictwem innego kanału komunikacji np. wiadomości

sms bądź podczas rozmowy telefonicznej przeprowadzonej po uprzednim zweryfikowaniu tożsamości adresata.

6. Użytkownik powinien zachować szczególną ostrożność podczas odbierania poczty elektronicznej, w szczególności - jeżeli nie ma pewności co do autentyczności adresata wiadomości - nie powinien otwierać plików i linków w niej zawartych, ani dołączonych załączników. Tego typu wiadomości, w większości przypadków mogą zawierać załączniki ze szkodliwym kodem, które po ich otwarciu infekują komputer Użytkownika a tym samym powodują realne ryzyko zaimplementowania kodu w pozostałych komputerach sieci wewnętrznej Jednostki.
7. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub ich zaszyfrowaniem przez kryptowirusy. W takim przypadku Użytkownik powinien niezwłocznie poinformować o zdarzeniu Administratora.
8. Użytkownik powinien regularnie przeglądać folder „Spam" i usuwać niepotrzebne wiadomości.

Art. 25. Zasady korzystania z Internetu

1. Użytkownik powinien korzystać z dostępu do sieci Internet wyłącznie w celach niezbędnych do wykonywania zadań służbowych.
2. Użytkownik nie powinien otwierać stron internetowych zawierających treści nie związane bezpośrednio z merytoryką pracy, ze względu na możliwość przypadkowego pobrania złośliwego kodu, który może automatycznie zainfekować system operacyjny komputera.
3. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane bez zgody Administratora.
4. Użytkownik nie może korzystać ze stron internetowych, na których prezentowane są treści o charakterze przestępczym, hackerskim, pornograficznym lub innym

zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla Użytkownika).

5. Użytkownik nie może pobierać aplikacji z sieci Internet bez wcześniejszej zgody Administratora.
6. Użytkownik, w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę internetową, powinien zwrócić uwagę na pojawienie się odpowiedniej ikony (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę „kłódki" i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Użytkownik powinien zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku) lub podania przez Internet jego loginów i haseł, PIN-ów, numerów kart płatniczych.

Art. 26. Zasady korzystania z bankowości elektronicznej

1. Użytkownik, który wykonuje przelewy bankowe zobowiązany jest do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem.
2. Użytkownik zobowiązany jest do zapamiętania lub przechowywania hasła dostępu oraz innych danych służących do uwierzytelniania i autoryzacji w bezpiecznym miejscu.
3. Użytkownik nie może opuścić stanowiska pracy bez wylogowania się i zamknięcia przeglądarki internetowej.
4. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.
5. W celu zalogowania się do systemu bankowości elektronicznej Użytkownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.
6. Obsługa informatyczna Jednostki jest zobowiązana do wyposażenia komputerów

służących do korzystania z bankowości elektronicznej w aktualne oprogramowanie oraz zabezpieczenia systemu na poziomie wysokim (m.in. oprogramowanie antywirusowe, włączony firewall) oraz do wykonywania okresowej kontroli zgodności ustawień sprzętu informatycznego z zasadami dotyczącymi bezpieczeństwa teleinformatycznego przekazanymi przez bank, który obsługuje bankowość elektroniczną.

7. Użytkownicy obsługujący bankowość elektroniczną są zobligowani do zapoznania się z zasadami bezpieczeństwa teleinformatycznego przekazanymi przez bank, który obsługuje bankowość elektroniczną.

Art. 27. Zarządzanie pojemnością przestrzeni dyskowej

1. W przypadku wdrażania nowej wersji oprogramowania przez Obsługę informatyczną Jednostki, konieczne jest uprzednie wykonanie niezbędnych kopii zapasowych zarówno użytkowanych systemów, jak i plików źródłowych poszczególnych Użytkowników – czyli wszystkiego co może być przydatne do zapewnienia poufności, integralności dostępności i rozliczalności.
2. Z każdej wdrożonej zmiany w wersji oprogramowania Obsługa informatyczna Jednostki jest zobowiązana sporządzić stosowną dokumentację tzw. bazę konfiguracji – raport (w wersji papierowej lub elektronicznej) pozwalającą na ewentualne przywrócenie systemów i oprogramowania do wersji sprzed zmiany, w której opisane są informacje na temat wykrytych nieprawidłowości, sugestie dot. procesu, uwagi (np. z raportów audytowych IT), które sugerują konieczność wdrożenia nowej wersji oprogramowania.
3. Co najmniej raz na pół roku Obsługa informatyczna Jednostki przeprowadza weryfikację sprzętu i oprogramowania oraz określa konieczność wprowadzenia zmian w oprogramowaniu, jeśli zaistnieje taka konieczność.

Art. 28. Zasady bezpiecznego przydzielania przestrzeni dyskowej

1. Podczas przydzielania przestrzeni dyskowej należy w sposób racjonalny przydzielać zasoby, zachowując próg ostrzegawczy na poziomie 80% zajętości przestrzeni.
2. Obsługa informatyczna Jednostki powinna wdrożyć mechanizmy umożliwiające w sposób racjonalny zarządzanie ww. przestrzenią dyskową dla każdego Użytkownika.
3. Raz na pół roku Obsługa informatyczna wykonuje analizę zajętości dysku. Do tego celu wykorzystuje wbudowane narzędzia konsoli zarządzania dyskami dostępnymi w systemach operacyjnych lub używa przeznaczonego do tego celu oprogramowania służącego do skanowania zajętości przestrzeni dyskowej.
4. W celu czyszczenia dysku ze zbędnych plików (pozostałości po działających lub odinstalowanych aplikacjach) oraz czyszczenia rejestru systemowego należy na przykład zainstalować przeznaczone do tego celu oprogramowanie, które po dokonaniu odpowiednich założeń systemowych dotyczących rozmiaru zbędnych plików umożliwi wyżej wskazane działania naprawcze.

Art. 29. Komunikacja i czynności serwisowe na odległość

1. Komunikacja z zewnątrz powinna być realizowana tylko poprzez mechanizmy szyfrujące zapewniające odpowiednie bezpieczeństwo (np. VPN, Team Viewer, AnyDesk). W przypadku podmiotów zewnętrznych dokonujących czynności serwisowych (np. aktualizacji oprogramowania dziedzinowego) dostęp taki jest nadzorowany przez Obsługę informatyczną Jednostki oraz każdorazowo powinien być poprzedzony autoryzacją (np. podaniem hasła do Team Viewer, które wygasa po skończonej sesji).
2. Komunikację należy prowadzić tylko za pomocą bezpiecznych metod transmisji, w tym włączenia transmisji szyfrowanej lub przeniesienia usług sieciowych na serwer posiadający taką możliwość.

Art. 30. Zasady pracy z urządzeniami mobilnymi

1. Administrator dopuszcza możliwość pracy z urządzeń mobilnych wyłącznie z urządzeń przeznaczonych do użytku służbowego.
2. Urządzenia mobilne służące do łączenia się systemami i sieciami zarządzanymi przez Administratora muszą być zgłoszone do Obsługi informatycznej Jednostki celem zabezpieczenia ich odpowiednimi środkami uwierzytelniania.
3. Administrator zabrania wykorzystywania służbowych urządzeń mobilnych do celów prywatnych oraz udostępniania ich osobom trzecim, jak również instalowania aplikacji, które nie są niezbędne do wykonywania obowiązków pracowniczych danego Użytkownika.
4. Administrator zabrania korzystania z publicznych sieci WiFi, chyba że połączenie jest dodatkowo zabezpieczone kanałem VPN oraz pozostawiania urządzenia bez nadzoru Użytkownika, w szczególności w miejscach ogólnodostępnych dla szerokiego grona osób trzecich.
5. Użytkownik nie może pozostawiać urządzenia mobilnego bez opieki, ani pożyczać go osobie trzeciej.
6. Z siecią służbową Użytkownik może łączyć się tylko za pośrednictwem urządzeń zaakceptowanych przez Administratora.
7. Użytkownik powinien używać tylko rozwiązań posiadające silne mechanizmy szyfrowania transmisji i ochrony danych.
8. Obsługa informatyczna Jednostki prowadzi ewidencję udostępnionych urządzeń mobilnych.

Art. 31. Zasady zabezpieczania sprzętu elektronicznego i systemu informatycznego

1. Komputery stacjonarne i przenośne powinny być zabezpieczone oprogramowaniem antywirusowym, które sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu.
2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich

usuwanie powinno odbywać się przy wykorzystaniu ww. oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych.

3. Obowiązkiem Obsługi informatycznej Jednostki jest nadzór nad aktualizacją oprogramowania antywirusowego.
4. Użytkownik jest obowiązany każdorazowo zawiadomić Obsługę informatyczną Jednostki o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.
5. Użytkownik, który posiada dostęp do systemów informatycznych powinien mieć zablokowaną możliwość instalowania nieautoryzowanego oprogramowania.

Art. 32. Zasady korzystania z elektronicznych nośników danych

1. Użytkownik może korzystać wyłącznie z szyfrowanych, elektronicznych nośników danych w szczególności pendrive'ów, dysków zewnętrznych, nośników optycznych przeznaczonych do użytku służbowego.
2. Użytkownik korzystający z elektronicznych nośników danych w całym okresie użytkowania odpowiedzialny jest za bezpieczeństwo danych. W przypadku zgubienia nośnika Użytkownik jest zobowiązany niezwłocznie powiadomić o tym fakcie Administratora.
3. Użytkownik korzystający z ww. urządzeń zobowiązany jest do:
   1) przechowywania danych na dysku szyfrowanym;
   2) transportu nośnika w sposób minimalizujący ryzyko kradzieży lub zniszczenia oraz stosownego jego zabezpieczenia przed uszkodzeniem;
   3) zdecydowanego i skutecznego uniemożliwienia skorzystania z nośnika osobom nieuprawnionym (np. rodzina, dzieci, znajomi).
4. Obsługa informatyczna Jednostki jest odpowiedzialna za prowadzenie inwentaryzacji sprzętu elektronicznego oraz utrzymywanie jej aktualności.

Art. 33. Zasady wykonywania przeglądów, serwisu i konserwacji sprzętu elektronicznego i nośników danych

1. Obsługa informatyczna Jednostki dokonuje przeglądu i konserwacji sprzętu elektronicznego i nośników danych.
2. Użytkownik nie może samodzielne dokonywać napraw sprzętu elektronicznego, wymiany jego podzespołów oraz wykonywać innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
3. W przypadku serwisowania infrastruktury teleinformatycznej przez podmioty zewnętrzne, Obsługa informatyczna Jednostki wymontowuje dyski twarde przed oddaniem ich do serwisu. W sytuacji, gdy do serwisu należy oddać cały zasób z dyskiem twardym, Administrator winien trwale usunąć wszystkie dane z dysku za pomocą certyfikowanych urządzeń. Jeżeli Administrator nie ma możliwości wymontowania dysku z urządzenia lub trwałego usunięcia danych, winien on podpisać stosowną umowę powierzenia danych z firmą serwisową.
4. Użytkownik ma obowiązek niezwłocznie powiadomić Obsługę informatyczną Jednostki o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
5. W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji Obsługa informatyczna Jednostki jest zobowiązana do:
   1) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych;
   2) oceny zasadności odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych, a w przypadku uzasadnionej konieczności - odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych.