POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. System ochrony danych osobowych.

1.1. Filary ochrony danych osobowych:

a. Legalność – Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
b. Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
c. Prawa Jednostki – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
d. Rozliczalność – Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

1.2. Zasady ochrony danych - Administrator przetwarza dane osobowe z poszanowaniem następujących zasad:

a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
b. rzetelnie i uczciwie (rzetelność);
c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
d. w konkretnych celach i nie „na zapas" (minimalizacja);
e. nie więcej niż potrzeba (adekwatność);
f. z dbałością o prawidłowość danych (prawidłowość);
g. nie dłużej niż potrzeba (czasowość);
h. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

1.3. Działania Administratora składające się na system ochrony danych:

a. Inwentaryzacja danych – Administrator dokonuje co najmniej raz w roku inwentaryzacji przetwarzanych przez siebie danych oraz stosowanych środków bezpieczeństwa.
b. Rejestry czynności przetwarzania danych – Administrator opracowuje i prowadzi rejestry czynności przetwarzania danych dla każdego wyodrębnionego i zidentyfikowanego procesu przetwarzania danych.
c. Bezpieczeństwo – Administrator zapewnia odpowiedni poziom zabezpieczenia danych osobowych poprzez wdrożenie organizacyjnych i technicznych środków bezpieczeństwa.
d. Obsługa praw jednostki – Administrator zapewnia realizację praw przysługujących osobom, których dane przetwarza.

1.4. Dokumenty wdrożone/stosowane przez Administratora z zakresu ochrony danych osobowych:

a. polityka przetwarzania danych osobowych;
b. rejestr czynności przetwarzania danych;
c. wstępne analizy ryzyka przetwarzania danych;
d. upoważnienia do przetwarzania danych osobowych;
e. rejestr upoważnionych pracowników;
f. umowy powierzenia przetwarzania danych;
g. rejestr podmiotów, którym powierzono przetwarzanie danych;
h. rejestr naruszeń danych osobowych;
i. informacje o przetwarzaniu danych osobowych;
j. raporty z audytu (inwentaryzacji) ochrony danych osobowych;

2. Szczegółowe procedury ochrony danych osobowych.

2.1. Przetwarzanie danych przez osoby upoważnione.

a. Dostęp do danych osobowych gromadzonych przez administratora mogą mieć wyłącznie osoby przez niego upoważnione.
b. Upoważnienie jest nadawane w formie pisemnej.
c. Upoważnienie powinno określać zakres danych, do których będzie miała dostęp osoba upoważniona oraz identyfikator (login) jeśli upoważnienie uwzględniać będzie dostęp do zbiorów elektronicznych.
d. Każda upoważniona osoba powinna zostać przeszkolona z zakresu aktualnych przepisów w dziedzinie ochrony danych osobowych i zapoznana z niniejszą polityką.

2.2. Przechowywanie dokumentów zawierających dane osobowe.

a. Przetwarzając dane osobowe w pisemnych dokumentach należy stosować następujące zasady:
   - pracować na dokumentach zawierających dane osobowe w taki sposób, aby osoba nieuprawniona nie miała do nich dostępu.
   - po skończeniu pracy zamykać szafy/pomieszczenia w których przechowujemy dokumenty zawierające dane osobowe;
   - okresowo sprawdzać stan archiwów;
   - wszystkie dokumenty przeznaczone do usunięcia, usuwać w sposób uniemożliwiający odczytanie danych przez osoby nieuprawnione;

2.3. Zasady pracy na komputerach służbowych.

a. Do pracy na komputerach służbowych dopuszczeni są wyłącznie użytkownicy upoważnieni do przetwarzania danych osobowych przez Administratora.
b. Każdy komputer służbowy powinien być zabezpieczony hasłem.
c. Komputery, z których korzysta więcej niż jeden użytkownik powinny mieć zindywidualizowane konta dla każdego użytkownika.
d. Użytkownik loguje się do komputera przez podanie identyfikatora (loginu) i wpisanie poprawnego hasła dostępu do systemu.
e. Identyfikatory (loginy) dla użytkowników administrator określa w upoważnieniach do przetwarzania danych osobowych.
f. Jeśli dane osobowe przetwarzane są w określonym programie (z wyłączeniem edytora tekstu i skrzynki mailowej) każdy użytkownik korzystający z tego programu powinien logować się do tego programu wykorzystując swój indywidualny login oraz hasło.
g. Po zakończeniu pracy na komputerze użytkownik zobowiązany jest każdorazowo do wylogowania się z systemu.
h. Administrator ustala następującą procedurę nadawania identyfikatorów oraz haseł:
   - administrator udzielając upoważnienia użytkownikowi określa dla niego indywidualny identyfikator (login) oraz podaje mu hasło do systemu, a w razie potrzeby także hasło do danego programu;
   - użytkownik zobowiązany jest samodzielnie uaktualniać hasła;
   - hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów;
   - hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
   - hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury;
   - hasło nie może być jednakowe z loginem użytkownika;
   - hasło powinno być unikalne, tj. takie, które nie było poprzednio stosowane przez pracownika;
   - hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie.
   - hasło musi być zmieniane przynajmniej dwa razy roku.

- w przypadku złamania poufności hasła, użytkownik zobowiązany niezwłocznie zmienić hasło i poinformować o tym fakcie administratora.
- hasła dostępu są tajne i ich ujawnianie jest bezwzględnie zabronione.
- w przypadku utraty przez użytkownika uprawnień do przetwarzania danych osobowych identyfikator oraz hasło do używanego przez tę osobę komputera powinny zostać natychmiast zmienione.

i. Użytkownikom zabrania się:

- instalowania oprogramowania bez wcześniejszej zgody Administratora,
- podłączania do komputera urządzeń nie będących własnością Administratora bez wcześniejszej zgody Administratora,
- zapisywania w pamięci komputera haseł dostępu.

j. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

k. Zewnętrzne nośniki pamięci (np. pendrive), na których zapisujemy dane osobowe w celu ich późniejszego zgrania na inny komputer powinny być odpowiednio zabezpieczone (hasło dostępu). Jeśli nie mamy takiej możliwości to powinniśmy zabezpieczyć dane, które zapisujemy na zewnętrznym nośniku pamięci.

2.4. Zasady korzystania z poczty służbowej.

a. Użytkownik korzystający z poczty służbowej jest zobowiązany do używania przypisanego mu adresu mailowego do wszelkiej korespondencji z innymi użytkownikami wewnątrz organizacji, klientami oraz innymi podmiotami w celach komunikacji służbowej.

b. Użytkownik może posługiwać się pocztą email wyłącznie w celach zgodnych z prawem, przestrzegając między innymi prawa autorskiego, praw własności intelektualnej oraz wszelkich innych przepisów, których złamanie mogłoby narazić Administratora na straty finansowe, wizerunkowe lub konsekwencje prawne.

c. Użytkownik nie może posługiwać się służbowym adresem email w celach prywatnych oraz rejestrować służbowego adresu poczty elektronicznej w serwisach internetowych niezwiązanych z wykonywaną pracą.

d. W przypadku uzyskiwania dostępu do poczty email z poza siedziby Administratora użytkownik zobowiązany jest do zachowania szczególnej ostrożności, w szczególności niedozwolone jest logowanie do systemów z:

- sieci ogólnodostępnych typu hotspot,
- komputerów ogólnodostępnych np. w hotelach, kawiarniach internetowych,
- komputerów współużytkowanych przez inne osoby (np. dzieci),
- komputerów co do których zachodzi podejrzenie że mogły zostać zainfekowane szkodliwym oprogramowaniem,

e. Podczas pracy z systemem pocztowym użytkownik zobowiązany jest do:

- zapewnienia poufności korespondencji poprzez ograniczenie wglądu do danych osób postronnych,
- nie otwierania i zapisywania załączników na komputerach pochodzących z nieznanych lub podejrzanych adresów.

2.5. Zasady sporządzania kopii zapasowych:

a. Zapasowe kopie bezpieczeństwa powinny być wykonywane przez każdego użytkownika przynajmniej raz w miesiącu, chyba że Administrator wdrożył oprogramowanie umożliwiające automatyczne sporządzanie kopii zapasowych.

b. Kopie bezpieczeństwa powinny być zapisywane na zewnętrznych dyskach pamięci lub tzw. chmurach.

c. Ewentualne dodatkowe kopie bezpieczeństwa należy przechowywać w innym miejscu niż kopie pierwotne.

d. Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.
e. Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie. Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.

2.6. Zgłaszanie naruszeń danych osobowych.

a. Każda osoba, która dostrzeże zagrożenie dla bezpieczeństwa danych osobowych Administratora lub będzie świadkiem naruszenia danych osobowych powinna natychmiast poinformować o tym Administratora.
b. Administrator powinien w ciągu 72 godzin, od stwierdzenia naruszenia zawiadomić Prezesa Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
c. Każde stwierdzone naruszenie Administrator odnotowuje w rejestrze naruszeń danych osobowych.
d. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   - niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   - niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   - nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek);
e. Do typowych naruszeń bezpieczeństwa danych osobowych należą:
   - zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   - zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
   - umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania);

Zatwierdzono przez: (podpisy)	Prezes Zarządu /-/ Krzysztof Kokoszkiewicz Wiceprezes Zarządu /-/ Stefan Kaszubski Zastępca Prezesa Zarządu /-/ Leszek Sułek
Data zatwierdzenia:	16.09.2020 r.