I. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osób odpowiedzialnych za te czynności.

1. Pracownikowi, którego zakres czynności zawiera dostęp do systemu informatycznego lub aplikacji, nadawane są uprawnienia dostępu z określeniem rodzajów danych oraz nadawany jest identyfikator stanowiący ciąg znaków, za pomocą którego użytkownik dokonuje procesu logowania.

   Nadanie (bezterminowo lub na czas określony) lub odebranie statusu użytkownika (również w przypadku ustania stosunku pracy) następuje na wniosek kierownika komórki organizacyjnej w oparciu o „Kartę-Upoważnienie", zwaną dalej „kartą użytkownika.".

   W karcie użytkownika kierownik komórki organizacyjnej dokonuje określenia: danych użytkownika, czasu obowiązywania uprawnień oraz szczegółowego wykazu uprawnień. **Nadane uprawnienia powinny być minimalne. Użytkownik powinien mieć dostęp do informacji tylko w takim zakresie, w jakim jest to niezbędne.**

2. Nadanie i odebranie statusu użytkownika następuje po złożeniu podpisu na karcie użytkownika przez właściwego Członka Zarządu – Dyrektora Pionu Spółki. Jeżeli zakres uprawnień obejmuje również przetwarzanie danych osobowych karta użytkownika jest zatwierdzana przez Prezesa Zarządu – Dyrektora Naczelnego, po uprzednim złożeniu podpisu przez właściwego Członka Zarządu – Dyrektora Pionu Spółki.

3. Nadanie uprawnień do przetwarzania danych osobowych wrażliwych może nastąpić po konsultacji Kierownika komórki organizacyjnej z Administratorem Bezpieczeństwa Informacji, który umieszcza swój podpis na karcie użytkownika, z adnotacją: „akceptuję" lub „nie akceptuję". Następnie karta użytkownika jest kierowana obiegiem zgodnie z zapisami punktu 2.

4. Użytkownik jest rejestrowany w systemie po przesłaniu oryginału karty użytkownika poprzez Administratora Systemów Informatycznych do Administratora Aplikacji. Administrator Aplikacji zakłada konto użytkownikowi, stosując identyfikator oraz hasło tymczasowe.

   Hasło podlega ochronie. **Za ochronę hasła odpowiada użytkownik**.

5. Oryginał karty użytkownika Administrator Aplikacji po wypełnieniu i nadaniu uprawnień użytkownikowi przesyła do Administratora Systemów Informatycznych, który wykonuje kopie i je przechowuje, umożliwiając do niej dostęp użytkownikowi. Administrator Bezpieczeństwa Informacji odbiera oryginały kart użytkownika, rejestruje je i przechowuje.
6. **Wzór karty-upoważnienia stanowi Załącznik do niniejszej Instrukcji.**
7. W przypadku braku miejsca w trakcie wypełniania karty użytkownika w zakresie szczegółowego wykazu uprawnień użytkownika dopuszcza się stosowanie dodatkowego załącznika.
8. W przypadku przesyłania danych osobowych sieciami publicznymi należy stosować metody kryptografii danych w uzgodnieniu z Administratorem Systemów Informatycznych.
9. Kierownik komórki organizacyjnej jest odpowiedzialny za przeszkolenie użytkownika w posługiwaniu się funkcjami/modułami/rolami w systemie, w zakresie niezbędnym do wykonywania obowiązków służbowych. W razie potrzeby, w trakcie szkolenia Kierownik komórki organizacyjnej powinien skorzystać z wiedzy i umiejętności Administratora Aplikacji.

9. Chcąc rozszerzyć lub zmodyfikować uprawnienia użytkownika, kierownik komórki organizacyjnej powinien postępować zgodnie z zasadami określonymi jak wyżej.
10. Zmiana uprawnień użytkownika w systemie informatycznym, w którym zaimplementowano mechanizm ról, powinna wiązać się z odebraniem starej roli użytkownikowi i nadaniu nowej.
11. Za udokumentowany okresowy przegląd (minimum 1 raz do roku) uprawnień użytkowników w systemie odpowiedzialni są kierownicy komórek organizacyjnych w porozumieniu z Administratorem Bezpieczeństwa Informacji.

II. Metody i środki uwierzytelnienia dostępu do danych oraz procedury związane z zarządzaniem i użytkowaniem.

1. Administrator Aplikacji w czasie zakładania konta nowego użytkownika (identyfikatora unikalnego w danym systemie) ustala pierwsze login i hasło, na które w systemie operacyjnym nałożony jest rygor zmiany przez użytkownika podczas pierwszego logowania.
2. Hasło jest przekazane użytkownikowi za pomocą poczty elektronicznej przez Administratora Aplikacji. Każde hasło wprowadzane przez użytkownika musi mieć minimum 8 znaków oraz zawierać małe i duże litery oraz cyfry. Odpowiednią postać hasła użytkownika wymusza aplikacja podczas zmiany hasła. Po 28 dniach (lub przy pierwszym poprawnym logowaniu) aplikacja wymusza na użytkowniku zmianę hasła. Jeżeli zmiana hasła nie nastąpi w czasie kolejnych 14 dni system blokuje konto użytkownika.
3. Niedopuszczalne jest zapisywanie i przechowywanie haseł w miejscach, które mogą być dostępne dla osób nieupoważnionych.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Podczas logowania się do systemu należy zwrócić uwagę, aby osoby nieupoważnione nie poznały naszego hasła. Wielokrotne próby niepoprawnego logowania powodują blokadę konta użytkownika. W razie potrzeby zakończenia pracy w systemie koniecznie należy zakończyć pracę w aplikacjach i wylogować się. Niedopuszczalne jest pozostawienie działającej aplikacji lub innych otwartych sesji w systemach bez nadzoru.
2. Podczas pracy w systemie należy zwracać szczególną uwagę na nieupoważnione osoby przebywające w bezpośredniej bliskości, które mogą mieć wgląd do danych wyświetlanych na monitorze i stosować takie ustawienie monitora, które na to nie pozwoli.
3. W celu zakończenia pracy należy: zakończyć pracę w aplikacjach i wylogować się. Wyłączanie terminala (komputera) przed zakończeniem pracy i wylogowaniem się jest niedopuszczalne.

4. O wszystkich problemach związanych z obsługą sprzętu i/lub aplikacji użytkownik powinien powiadomić przełożonego i Służby Informatyczne.
5. O fakcie zapomnienia hasła do własnego konta użytkownik zobowiązany jest poinformować kierownika komórki organizacyjnej, a ten skontaktować się z Administratorem Systemów Informatycznych. Po nadaniu nowego hasła postępuje się jak w przypadku pierwszego hasła. Niedopuszczalne jest przekazywanie własnego identyfikatora (loginu) i hasła innej osobie. Niedopuszczalna jest praca z wykorzystaniem loginu innego pracownika.
6. W przypadku uzasadnionego podejrzenia naruszenia bezpieczeństwa systemu (np. fakt poznania hasła przez osobę nieupoważnioną), użytkownik zobowiązany jest powiadomić bezpośredniego przełożonego i Administratora Systemów Informatycznych.

IV. Procedury tworzenia kopii zapasowych danych i aplikacji.

Kopie awaryjne danych wykonywane są na serwerach przez Służby Informatyczne. Sposób tworzenia i harmonogram wykonywania kopii zapasowych przedstawiony jest w części niejawnej Polityki Bezpieczeństwa Informacji.

V. Sposób i miejsce przechowywania oraz transport nośników z danymi i kopii zapasowych.

Sposób i miejsce przechowywania oraz transport nośników z danymi i kopii zapasowych jest opisany w części niejawnej Polityki Bezpieczeństwa Informacji.

VI. Sposoby zabezpieczania systemów informatycznych przed działaniem oprogramowania mającego na celu nieuprawniony dostęp.

1. Sposoby zabezpieczania systemów informatycznych przed działaniem oprogramowania mającego na celu nieuprawniony dostęp są opisane w części niejawnej Polityki Bezpieczeństwa Informacji.
2. Dla wszystkich użytkowników stosowany jest system kontroli i upoważnień dostępu do sieci zewnętrznej, kontroli ruchu danych.

VII. Realizacja wymogów § 7 ust. 1 pkt 4 rozporządzenia.

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym system ten zapewnia odnotowanie, sporządzanie i wydrukowanie raportu:
   - daty pierwszego wprowadzenia danych do systemu,
   - identyfikatora użytkownika wprowadzającego dane osobowe do systemu,
   - źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,
   - informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,
   - sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.
2. Odnotowanie informacji, o dacie pierwszego wprowadzenia danych i o identyfikatorze użytkownika wprowadzającego dane osobowe do systemu informatycznego następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

VIII. Procedury przeglądów i konserwacji systemów.

1. Wszystkie zabiegi konserwacyjne i przeglądy stanu baz danych i systemów plików wykonuje Administrator Aplikacji. Okresowe konserwacje baz danych i systemu plików są elementem codziennego i comiesięcznego archiwum i są wykonywane przez Administratora Aplikacji.
2. W przypadku koniecznej obecności pracowników firm zewnętrznych (np. instalacje,

konfiguracje nowych produktów) przy pracach związanych z możliwym dostępem do danych osobowych i informacji wrażliwych, konieczna jest stała obecność i nadzór Administratora Aplikacji lub pracownika wyznaczonego przez Administratora Systemów Informatycznych.

3. W przypadku konieczności naprawy sprzętu mogącego zawierać dane osobowe, poza budynkiem podanym w Załączniku Nr 2 Administratora Aplikacji, jego upoważnieni pracownicy wykonują odpowiednie czynności związane z pozbawieniem nośników informacji danych w taki sposób, aby uniemożliwić jej odzyskanie i odczyt.

*** Instrukcja dotyczy zarządzania systemami informatycznymi:**

- autorstwa CENTRUM INFORMATYKI Sp. z o.o., ul. Bałuckiego 4, 43-100 Tychy (system ISKP, ISSW),
- autorstwa innych firm, których administrację prowadzi Administrator Aplikacji, którym jest zgodnie z podpisanymi umowami CENTRUM INFORMATYKI Sp. z o.o. (FKX, GMX – firmy Prokom).

- Koniec-