Wzór procedury korzystania z systemów informatycznych, kontroli dostępu, ich aktualizacji oraz szyfrowania danych osobowych wynoszonych lub przesyłanych poza siedzibę Kancelarii.

Wstęp.

1.1. Cel i zakres

1.1.1. Niniejszy dokument (dalej „Procedura") określa podejście Kancelarii do zarządzania Systemami informatycznymi oraz ustanawia mechanizmy kontrolne i zasady korzystania z Systemów informatycznych.
1.1.2. Procedura podlega okresowym, co najmniej rocznym przeglądom i aktualizacjom, zwłaszcza w przypadku istotnych zmian w organizacji, procesach lub wykorzystywanego przez Kancelarię oprogramowania lub sprzętu..
1.1.3. Każdy partner, pracownik oraz współpracownik Kancelarii jest zobowiązany do przestrzegania niniejszej Procedury oraz wszelkich innych regulacji wewnętrznych obowiązujących w Kancelarii, które są związane z Procedurą.

1.2. Słownik pojęć

1.2.1. Osoba trzecia – osoba fizyczna, osoba prawna lub inna osoba nie posiadająca osobowości prawnej upoważniona przez Kancelarię, na podstawie odpowiednich przepisów prawa, umów lub zgód, do przetwarzania danych Kancelarii.
1.2.2. Systemy informatyczne – zbiór procesów, zasobów technicznych, zasobów fizycznych i ludzkich, regulacji, narzędzi i mechanizmów wykorzystywanych do przetwarzania informacji.
1.2.3. Uprawnienia administratora (Privileged User Rights) – najwyższy poziom uprawnień, który pozwala użytkownikowi na instalowanie i modyfikowanie oprogramowania oraz zmianę ustawień konfiguracyjnych.
1.2.4. Użytkownik – osoba, która ma dostęp do Systemu informatycznego Kancelarii posiadająca określone uprawnienia, adekwatnych do pełnionej funkcji w Kancelarii .
1.2.5. Zasada najmniejszych uprawnień – to praktyka ograniczania dostępu do minimalnego poziomu, który pozwoli na wystarczające dla danego Użytkownika korzystanie z Systemu informatycznego w celu wykonywania powierzonych obowiązków.
1.2.6. Zasób informacyjny – wszystko, co ma wartość materialną i/lub niematerialną oraz może zostać uznane za aktywa Kancelarii, a także dane powierzone Kancelarii. Zasoby informacyjne mogą obejmować informacje, procesy biznesowe, sprzęt, oprogramowanie, budynki / pomieszczenia, zasoby ludzkie, sieci informatyczne, itp.

1.3. Role i obowiązki (zależnie od ról i obowiązków ustanowionych w Kancelarii).
1.3.1. Partner Zarządzający / Zarząd
1.3.2. Dyrektor Działu IT
1.3.3. Dyrektor Administracyjny
Odpowiedzialny za:

- opracowywanie, przegląd i aktualizacje Procedury,
- zapewnienie, że wszyscy partnerzy, pracownicy przestrzegają Procedury,
- zapewnienie przestrzegania tej Procedury przez podmioty zewnętrzne współpracujące lub zatrudnione przez Kancelarię.

Korzystanie z systemów informatycznych.

2.1. Zasady ogólne

2.1.1. Systemy informatyczne powinny być wykorzystywane wyłącznie do celów określonych przez Kancelarię.

2.1.2. Wszelkie czynności Użytkowników w Systemach informatycznych, które nie zostały dopuszczone przez przełożonego danego Użytkowania, a które nie polegają na wykonywaniu zadań Kancelarii, są zabronione.

2.1.3. Wykorzystywanie Zasobów informacyjnych do celów prywatnych reguluje paragraf „2.6. Prywatne wykorzystanie zasobów informacyjnych".

2.1.4. Użytkownikom Systemu informatycznego nie wolno podejmować jakichkolwiek działań umyślnie mających na celu:

- naruszenie prawa,
- obrażanie lub nękanie innych osób,
- uszkadzanie lub niszczenie danych Kancelarii,
- obniżenie wydajności Systemu informatycznego lub poziomu jego bezpieczeństwa,
- nieuprawnione rozpowszechnianie jakichkolwiek informacji chronionych prawem, w tym prawem autorskim,
- przesyłanie danych zawierających złośliwy kod (wirusy, trojany, robaki itp.),
- przekazywanie poufnych danych osobom trzecim bez odpowiedniego upoważnienia,
- przetwarzanie danych, które mogą mieć negatywny wpływ na reputację Kancelarii (np. treści o charakterze pornograficznym, propagujących ruchy ekstremistyczne, terroryzm, lub dyskryminujące w szczególności ze względu na płeć, rasę, pochodzenie etniczne, narodowość, religię, wyznanie, światopogląd, niepełnosprawność, wiek lub orientację seksualną),
- łamanie zabezpieczeń Systemu informatycznego.

2.1.5. W przypadku naruszenia Procedury przez pracownika, takie naruszenie może skutkować postępowaniem dyscyplinarnym.

2.1.6. W przypadku naruszenia Procedury przez Osobę trzecią, takie naruszenie może skutkować podjęciem kroków prawnych na podstawie przepisów prawa lub istniejących zobowiązań.

2.2. Dostęp do systemów informatycznych.

2.2.1. Dostęp do Systemu informatycznego wymaga odpowiedniego zatwierdzenia i autoryzacji przez uprawnioną osobę w Kancelarii.

2.2.2. Dostęp do Systemów Informacyjnych odbywa się na podstawie loginu i hasła. W przypadku dostępu zdalnego do Zasobów informacyjnych Kancelarii zapewniona jest funkcjonalność wieloetapowego uwierzytelnienia (tzw. MFA).

2.2.3. Każdemu Użytkownikowi nadawany jest indywidualny login i hasło.

2.2.4. Login użytkownika musi składać się z unikalnego ciągu znaków.

2.2.5. Login jest przypisany tylko do jednej osoby i nie może być udostępniany innym Użytkownikom.

2.2.6. Wszystkie Systemy informatyczne muszą zapewnić właściwe uwierzytelnienie tożsamości Użytkowników uzyskujących do nich dostęp, przed rozpoczęciem sesji.

2.2.7. Każdy Użytkownik odpowiada za wszelkie czynności dokonywane przez niego w Systemie informatycznym. Każdą operację wykonaną po zalogowaniu uważa się za dokonaną przez właściciela loginu.

2.2.8. Użytkownicy zobowiązani są do zachowania w tajemnicy haseł do Systemów informatycznych.
2.2.9. Dostęp do Systemów informatycznych powinien być przydzielany w oparciu o zasadę minimalnego uprzywilejowanego, biorąc pod uwagę obowiązki danego Użytkownika.
2.2.10. Nieautoryzowane próby uzyskania dostępu do Systemów informatycznych są zabronione.
2.2.11. Każdy Użytkownik Systemu informatycznego w celu korzystania z niego zobowiązany jest do przeprowadzenia procesu identyfikacji i uwierzytelniania (tzw. logowania).
2.2.12. Użytkownicy nie mogą udostępniać loginu i haseł innym Użytkownikom i nie powinni umożliwiać innym Użytkownikom wykonywania czynności na ich kontach.
2.2.13. Konta grupowe muszą być używane tylko wtedy, gdy inne rozwiązania nie są możliwe i jeśli korzystanie z takiego konta zostało zatwierdzone przez Zarząd / Partnera zarządzającego.

2.3. Uprawnienia administratora (Privileged User Rights).
2.3.1. Uprawnienia administratora do Systemów informatycznych (np. konta administracyjne dla systemów operacyjnych, baz danych lub aplikacji, które mogą obejść ich kontrolę dostępu) powinny być przyznawane tylko Użytkownikom, którzy wymagają takich uprawnień ze względu na wykonywane obowiązki służbowe.
2.3.2. Każde konto ogólne (np. konto gościa, konta domyślne) po zakończeniu uprawnionej sesji należy usunąć lub zablokować. Jeśli jest to możliwe, nazwy takich kont powinny zostać zmienione.
2.3.3. Zgody na nadanie uprawnień administratora udziela Zarząd / Parter zarządzający.
2.3.4. Hasło do konta root jest przechowywane w zapieczętowanej kopercie w zamykanym na klucz pokoju lub w sejfie, do którego dostęp ma tylko Zarząd / Parter zarządzający.
2.3.5. Wszystkie hasła do usług zewnętrznych i innych elementów infrastruktury IT (np. routerów) są przechowywane przez uprawnione osoby i poza osobami uprawnionymi żadna inna osoba nie ma do nich dostępu.
2.3.7. Uprawnienia administratora powinny zostać odebrane, gdy tylko dostęp przestanie być niezbędny do wykonywania obowiązków służbowych.
2.3.8. Administratorzy nie mogą definiować żadnych czynności związanych z:
- procesem projektowania mechanizmów kontroli bezpieczeństwa Systemu informatycznego,
- procesem zatwierdzania mechanizmów kontroli bezpieczeństwa Systemu informatycznego,
- monitorowaniem pracy innych Administratorów.

2.4. Kontrola dostępu do sieci.
2.4.1. Dostęp pochodzący spoza sieci firmowej Kancelarii do jej sieci wewnętrznej musi być dodatkowo uwierzytelniany poza kombinacją nazwy użytkownika i hasła (np. za pomocą tokenów lub innych urządzeń, aplikacji autentykacyjnej, jednoarowych kodów uwierzytelniających lub uwierzytelnieniu opartym na certyfikacie bezpieczeństwa).
2.4.2. Bramy sieciowe powinny być zaimplementowane w celu ograniczenia dostępu do sieci do następujących typów aplikacji lub usług:
- systemy przesyłania wiadomości,
- transfery plików,
- aplikacje internetowe.

2.4.3. Jeśli jest to technicznie możliwe, wszystkie połączenia między sieciami firmowymi a Internetem powinny przechodzić przez serwer proxy aplikacji i być sprawdzane pod kątem adresów źródłowych i docelowych.
2.4.4. Połączenia sieciowe z Internetu muszą być zabezpieczone tzw. fire wall'em, aby zapobiec nieautoryzowanemu dostępowi do sieci Kancelarii.
2.4.5. Serwery z protokołami, które umożliwiają przekazywanie pakietów danych lub pozwalających na zmianę trasy (re-routing), należy skonfigurować tak, aby nie zezwalały na tę funkcję, chyba że jest to niezbędne dla wykonywania zadań Kancelarii. Na przykład „przekazywanie IP" i „pasywna" funkcja FTP powinny być wyłączone.
2.4.6. Adresy IP sieci wewnętrznej Kancelarii nie powinien być widoczne dla połączeń z zewnętrz sieci Kancelarii.
2.4.7. Usługi sieciowe w systemach powinny być wyłączone, chyba że jest to niezbędne dla wykonywania zadań Kancelarii.
2.4.8. Porty i usługi informatyczne, które nie obsługują zadań Kancelarii, powinny być wyłączone (zablokowane).
2.4.9. Niedozwolone jest podłączanie do infrastruktury IT Kancelarii jakiegokolwiek prywatnego sprzętu bez uprzedniej zgody uprawnionego do wyrażenia takiej zgody pracownika Kancelarii.

2.5. Korzystanie z Oprogramowania.
2.5.1. Dozwolone jest instalowanie oprogramowania, które zostało zatwierdzone przez Zarząd / Partnera zarządzającego.
2.5.2. Instalację i konfigurację oprogramowania wykonuje Administrator Systemu Informatycznego.
2.5.3. Wszystkie stacje robocze powinny być skonfigurowane w taki sposób, aby żadne oprogramowanie nie mogło być instalowane bezpośrednio przez Użytkownika.
2.5.4. Niedozwolone jest dokonywanie nieautoryzowanych zmian w Systemie informatycznym.
2.5.5. Użytkownikom Systemu informatycznego nie wolno podejmować prób uzyskania uprawnień Użytkowników uprzywilejowanych (Privileged User Rights).
2.5.6. Oprogramowanie może być użytkowane tylko zgodnie z zakupioną licencją i zgodnie z przepisami prawa.
2.5.7. Zabronione jest uruchamianie jakichkolwiek plików instalujących oprogramowanie z nośników danych (CD/DVD/USB/mobile), pobranych z Internetu lub jakichkolwiek załączników do wiadomości e-mail, chyba że zostały one zeskanowane programem antywirusowym.

2.6. Prywatne wykorzystanie Zasobów informacyjnych.
2.6.1. Przez prywatne korzystanie z Zasobów informacyjnych Kancelarii należy rozumieć każdą czynność wykonywaną przez Użytkownika na Zasobach informacyjnych Kancelarii, która nie jest związana z zadaniami Kancelarii.
2.6.2. Prywatne korzystanie z Zasobów informacyjnych jest dozwolone dla Użytkowników tylko w następujących sytuacjach:

- nie wpływa negatywnie na poziom bezpieczeństwa Zasobów informacyjnych,
- nie narusza żadnych innych regulacji wewnętrznych Kancelarii,
- nie wpływa negatywnie na wydajność i terminowość pracy osób zatrudnionych w Kancelarii,

- nie wpływa negatywnie na wydajność Systemów informatycznych,
- nie jest wykorzystywane do jakiejkolwiek prywatnej działalności gospodarczej lub biznesowej innej niż prowadzona we współpracy z Kancelarią.

2.6.3. Użytkownik może używać dedykowanego folderu do celów prywatnych, w którym może przechowywać pliki (za wyjątkiem plików instalujących oprogramowanie) .
2.6.4. Zabrania się udostępniania kont e-mail Kancelarii do celów prywatnych i prywatnych kont e-mail do celów związanych z wykonywaniem zadań Kancelarii.
2.6.5. Użytkownik ponosi pełną odpowiedzialność za korzystanie z Zasobów Systemu informatycznego w celach prywatnych.

2.7. Poczta elektroniczna (e-mail).
2.7.1. Firmowe konto e-mail powinno być wykorzystywane tylko do celów służbowych zgodnie z punktem 2.6.
2.7.2. Z firmowego konta e-mail należy korzystać zgodnie z następującymi zasadami:
- konto powinno być wykorzystywane w sposób zapewniający bezpieczeństwo informacji i chroniących reputację Kancelarii,
- treść e-maili nie powinna nikogo obrażać i nie powinna naruszać żadnych innych regulacji wewnętrznych Kancelarii,
- Użytkownicy powinni zachować szczególną uwagę w przypadku otrzymania wiadomości e-mail z nieznanego, podejrzanego źródła (domeny zewnętrznej) – takich wiadomości nie należy otwierać,
- Użytkownicy nie powinni przekazywać e-maili związanych z działalnością Kancelarii do nieautoryzowanych odbiorców,
- Użytkownicy nie powinni celowo wysyłać wiadomości e-mail zawierających złośliwy kod lub spam,
- Użytkownicy nie powinni uruchamiać żadnych plików instalujących oprogramowanie dołączanych do wiadomości e-mail,
- Użytkownicy nie powinni ujawniać adresu e-mail osobom trzecim bez biznesowego uzasadnienia, ze względu na ryzyko otrzymywania spamu.

2.8. Internet.
2.8.1. Zabrania się przeglądania stron internetowych, które mogą zostać uznane za obraźliwe lub zawierających treści mogące naruszać prawo lub dobre obyczaje.
2.8.2. Dyrektor Działu IT (lub inna uprawniona osoba) określa zakres i rodzaj narzędzi wykorzystywanych do dostępu do Internetu (przeglądarki stron internetowych) oraz określa jego bezpieczną konfigurację.
2.8.3. Logi z serwerów proxy są przechowywane na zewnętrznym serwerze.
2.8.4. Użytkownikom Systemu informatycznego nie wolno pobierać, otwierać, instalować, przechowywać ani wysyłać plików, które pochodzą z niezaufanych, niebezpiecznych stron internetowych i nie są związane z obowiązkami związanymi z wykonywaniem zadań przez Kancelarię.
2.8.5. Media społecznościowe, blogi lub inne zewnętrzne usługi internetowe (np. fora internetowe itp.) nie mogą być wykorzystywane do oficjalnego przetwarzania informacji związanych z działalnością Kancelarii, chyba że Zarząd / Partner zarządzający wyrazi na to zgodę.
2.8.6. W przypadku korzystania z serwisów, o których mowa w pkt. 2.8.5. Użytkownicy zobowiązani są do zachowania poufności informacji dotyczących innych pracowników i

współpracowników Kancelarii lub innych Użytkowników Systemu informatycznego, w szczególności nie powinni:
- przesyłać lub publikować jakichkolwiek treści, które mogą podważyć reputację Kancelarii lub jej partnerów i pracowników,
- przesyłać lub publikować jakichkolwiek treści i, które mogą być wykorzystane do identyfikacji Użytkownika Systemu informatycznego (np. oficjalny e-mail, numer telefonu, numer identyfikacyjny itp.), chyba że Zarząd / Partner zarządzający wyrazi na to zgodę.

2.9. Zarządzanie hasłami.
2.9.1. W systemach informatycznych należy stosować następujące ustawienia haseł:
- minimalna długość hasła (ilość znaków): co najmniej 12
- pierwsze logowanie przy użyciu hasła jednorazowego: Tak
- skład hasła: (np. alfanumeryczne, znaki specjalne) wielkie litery, cyfry
- częstotliwość wymuszonych zmian hasła: (*do decyzji)*
- nieudane próby logowania przed blokadą (dla stacji roboczych Użytkowników i Administratorów): 5
- możliwość nadawania przez Użytkowników własnych haseł :Tak
- historia haseł (liczba haseł): 3
- sesja bezczynna: limit czasu 15 min
- rejestrowanie nieudanych prób logowania: Tak

2.9.2. Początkowe hasło do logowania nie może być łatwo kojarzone z Użytkownikiem (np. numer PESEL, numer identyfikacyjny pracownika, adres, numeryczny odpowiednik nazwiska itp.).
2.9.3. Każdy Użytkownik Systemu informatycznego otrzymuje od Administratora jednorazowe hasło do wstępnego logowania. Hasło może zostać ujawnione tylko danemu Użytkownikowi.
2.9.4. Hasło nie powinno być wyświetlane podczas wprowadzania i nie powinno być przesyłane w postaci zwykłego tekstu w wiadomości e-mail.
2.9.5. Hasło powinno być możliwe do zapamiętania, ale trudne do odgadnięcia. Nie powinien zawierać informacji, które można łatwo powiązać z Użytkownikiem m.in. imię, nazwisko, numer telefonu, data urodzenia, imiona członków rodziny, itp.
2.9.6. Hasło powinno być inne niż login lub być ciągiem kolejnych cyfr lub liter nawet wpisanych na klawiaturze (np. 123456, qwerty itp.).
2.9.7. Hasło powinno być odporne na ataki słownikowe. Nie powinno składać się ze słów, które można łatwo znaleźć w słownikach haseł.
2.9.8. Pozostawione bez nadzoru Systemy informatyczne powinny być zabezpieczone przed nieautoryzowanym dostępem za pomocą mechanizmów kontroli dostępu, takich jak blokada ekranu po określonym czasie bezczynności.
2.9.9. Użytkownicy powinni zawsze wylogować się ze wszystkich Systemów informatycznych i aplikacji, gdy skończą z nich korzystać.
2.9.10. Karta dostępu jest używana w godzinach pracy jako jedyny sposób wejścia do Kancelarii.
2. 9.11. Karta dostępu i PIN służą do wejścia do Kancelarii po godzinach pracy oraz do wejścia do serwerowni i archiwum.
2.9.12. Kody PIN powinny składać się z co najmniej 4 cyfr, które nie powinny być ciągiem kolejnych cyfr.

2.9.13. Elementy uwierzytelniające, takie jak hasła i kody PIN, nie powinny być ujawniane żadnemu innemu Użytkownikowi ani Osobie Trzeciej.
2.9.15. Hasła używane przez Administratorów muszą być przechowywane przy zachowaniu szczególnej staranności w sposób zapewniający poufność.
2.9.16. Hasła nie powinny być przechowywane ani zapisywane na papierze, w pliku, na urządzeniu mobilnym, w makrach lub funkcjach, chyba że Dyrektor IT (lub inna uprawniona osoba) zatwierdzi daną metodę przechowywania haseł.
2.9.17. W przypadku podejrzenia ujawnienia hasła lub naruszenia bezpieczeństwa Systemów informatycznych Użytkownik jest zobowiązany do niezwłocznej zmiany hasła i zgłoszenia incydentu przełożonemu.
2.9.18. Dozwolone jest uzgodnienie wyjątków od ww. regulacji zarządzania hasłami, jeżeli Zarząd / Partner zarządzający wyrazi na to zgodę.

2.10. Dostęp zdalny.
2.10.1. Zdalny dostęp do Systemu informatycznego Kancelarii powinien być możliwy tylko po pomyślnej identyfikacji i autoryzacji Użytkownika.
2.10.2. Zdalny Dostęp do Systemów informatycznych może być udzielony wyłącznie Użytkownikom, którzy wymagają takiego dostępu ze względu na zakres swoich obowiązków, z tytułu zawartej umowy lub na podstawie zgody udzielonej przez Zarząd / Partnera zarządzający.
2.10.3. W przypadku dostępu zdalnego do Zasobów informacyjnych Kancelarii zapewniona jest funkcjonalność wieloetapowego uwierzytelnienia (tzw. MFA)
2.10.4. W celu korzystania ze Zdalnego dostępu należy również spełnić następujące warunki techniczne:

- każdy port używany do zdalnego dostępu powinien być zabezpieczony,
- system operacyjny i oprogramowanie antywirusowe na urządzeniu z którego korzysta Użytkownik do zdalnego dostępu jest zainstalowane w najbardziej aktualnej wersji,
- włączona jest automatyczna aktualizacja programu antywirusowego.

2.11. Rejestrowanie i monitorowanie.
2.11.1. Funkcjonalność rejestrowania zdarzeń w Systemie informatycznym powinna jest zapewniona.
2.11.2. Działania Administratorów jest rejestrowane w dziennikach zdarzeń Systemu informatycznego.
2.11.3. Działania Użytkowników uznane za istotne z punktu widzenia bezpieczeństwa informacji powinny być rejestrowane w dziennikach zdarzeń Systemu informatycznego.
2.11.5. Dla każdego Systemu informatycznego należy zdefiniować częstotliwość przeglądania dzienników zdarzeń oraz listę pracowników, którzy mają dostęp tylko do odczytu do dzienników zdarzeń.
2.11.6. Dzienniki zdarzeń muszą zawierać co najmniej następujące informacje niezależnie od systemu generującego dziennik, chyba że nie jest to technicznie możliwe:

- data i godzina zdarzenia (czas w formacie UTC),
- identyfikator użytkownika osoby wykonującej czynność,
- rodzaj zdarzenia,
- nazwa zasobu, którego dotyczy zdarzenie
- rodzaj zdarzenia (np. usunięcie, modyfikacja itp.),

- informacja o udanym lub nieudanym wykonaniu operacji na danych,
- źródło zdarzenia (tj. terminal, port, lokalizacja, IP, nazwa hosta itp.).

2.11.7. Dzienniki zdarzeń należy przeglądać w szczególności, gdy wystąpi następująca sytuacja:
- krytyczna awaria systemu informatycznego,
- miała miejsce próba obejścia zabezpieczeń Systemu informatycznego,
- doszło do incydentu związanego z niedostępnością Systemu informatycznego,
- miało miejsce nadzwyczajne zwiększenie transmisji danych lub przeciążenie systemu.

2.11.8. Dane zapisane w dziennikach zdarzeń powinny być archiwizowane i przechowywane przez co najmniej 6 miesięcy.
2.11.9. W celu zapewnienia ochrony logi zdarzeń powinny być przechowywane na serwerze zewnętrznym.
2.11.10. Archiwum dzienników zdarzeń Systemu informatycznego powinno być chronione przed nieuprawnionym dostępem, a dostęp do zewnętrznego serwera dziennika powinien być ograniczony.
2.11.11. Wyznaczonej osobie należy zapewnić dostęp tylko do odczytu do zewnętrznego serwera dziennika zdarzeń w celu dokonywania przeglądów.
2.11.12. Systemy informatyczne uważane za krytycznie ważne dla działania Kancelarii powinny dokonywać transferu dzienników zdarzeń w czasie rzeczywistym na zewnętrzny serwer dzienników.
2.11.13. Zegary wszystkich Systemów informatycznych powinny być zsynchronizowane z uzgodnionym dokładnym źródłem czasu.
2.11.14. Synchronizacja zegara powinna być wykonywana przez Dyrektora ds. IT (lub inną uprawnioną osobę) corocznie i każdorazowo dokumentowana.

3. Szyfrowanie danych osobowych wyniesionych poza siedzibę Kancelarii

3.1. W przypadku wynoszenia na nośnikach danych lub przesyłania poza System informatyczny Kancelarii danych osobowych powinny być one odpowiednio zabezpieczone.
3.2. Przez odpowiednie zabezpieczenie należy rozumieć w szczególności ochronę plików zawierających dane osobowe przed otworzeniem lub modyfikacją za pomocą hasła.
3.3. Urządzenia (stacje robocze, laptopy, smartfony itp.) powinny być zabezpieczone przed uzyskaniem dostępu przez osobę nieuprawnioną tylko po pomyślnej identyfikacji i autoryzacji Użytkownika z zachowaniem funkcjonalności wieloetapowego uwierzytelnienia (tzw. MFA).

4. Zarządzanie aktualizacjami

4.1. Dyrektor ds. IT (lub inna osoba wskazana przez Zarząd / Partnera zarządzającego) zapewniają regularne aktualizowanie oprogramowania wykorzystywanego przez Kancelarię zgodnie z zaleceniami producenta.
4.2. Oprogramowanie, które nie jest wspierane przez producenta nie powinno być wykorzystywane w Kancelarii, chyba że jest to niezbędne do wykonywania zadań Kancelarii i zostało zatwierdzone przez Zarząd / Partnera zarządzającego. W przypadku korzystania z oprogramowania nie wspieranego przez producenta Kancelaria zapewnia, w miarę technicznych możliwości, odseparowanie urządzeń na których uruchamiane jest niewspierane oprogramowanie od reszty infrastruktury Systemu informatcznego.

4.3. Dyrektor IT (lub inna osoba wskazana przez Zarząd / Partnera zarządzającego) zapewnia regularny, nie rzadziej niż raz na kwartał, przegląd aktualizacji wykorzystywanego oprogramowania.