Ministerstwo Cyfryzacji

Polityka Bezpieczeństwa Informacji dla systemu mObywatel

(wyciąg)

Metryka dokumentu

Właściciel	Minister właściwy ds. informatyzacji			
Tryb zatwierdzenia:	Dokument zatwierdza Dyrektor, Ministerstwo Cyfryzacji			
Stan	Do akceptacji przez MC	Daty obowiązywania		
Założenia	Dokument stanowi załącznik do Polityki Bezpieczeństwa Informacji dla systemu mObywatel			
Adresaci	Uprawnieni Interesariusze systemu mObywatel			
Historia dokumentu	Wersja	Data	Autor	Opis zmian
	0.2	30.07.2019	Zespół ZBT COI	Utworzenie dokumentu

Spis treści

1. Cel

Celem niniejszego dokumentu jest wskazanie najważniejszych zasad obowiązujących w zakresie zarządzania bezpieczeństwem informacji systemu mObywatel oraz uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów rozumiane jako zapewnienie poufności, integralności i dostępności zasobów, a także zapewnienie rozliczalności podejmowanych działań.

Przedmiotowy dokument stanowi wyciąg z dokumentu zasadniczego, jakim jest Polityka Bezpieczeństwa Informacji dla systemu mObywatel (zamiennie PBI) i stanowi kompendium podstawowej wiedzy z zakresu systemu zarządzania bezpieczeństwem informacji oraz przeznaczony jest dla wskazanych użytkowników systemu.

Przedmiotem dokumentu jest określenie kluczowych zasad dotyczących zapewnienia bezpieczeństwa informacji (danych) mObywatel, obejmujących zabezpieczenia:

- organizacyjne obszaru zawierającego dane (informacje) podlegające ochronie,
- techniczne systemów informacyjnych zawierających dane podlegające ochronie,

w zakresie:

- aktywów systemu,
- postępowania z informacją,
- postępowania z incydentami bezpieczeństwa informacji,
- zarządzanie ryzykiem,
- monitoringu i nadzoru nad zmianą.

2. Opis systemu

System mObywatel to system umożliwiający użytkownikom (m.in. obywatelom, podmiotom) korzystanie z odpowiedniego oprogramowania instalowanego na urządzeniu mobilnym w celu potwierdzania i weryfikacji tożsamości. Jednym z podstawowych założeń jest możliwość udostępniania dokumentów w trybie offline.

System ten pozwala na potwierdzanie tożsamości wszędzie tam, gdzie wystarczy okazać swój dokument ze zdjęciem oraz nie jest wymagane posiadanie dowodu osobistego czy paszportu. Wszystkie pobrane i udostępniane dane są przechowywane w zaszyfrowanej formie na urządzeniu mobilnym.

System mObywatel umożliwia obywatelom dostęp do swoich danych i bezpiecznego ich przesyłania w celach weryfikacyjnych do zainteresowanych stron. Przyjęte modele obejmują wymianę:

a. obywatel do obywatela:
   - jednostronne przekazanie danych lub
   - obustronna wymiana danych,

b. obywatel do przedsiębiorstw,

c. obywatel do administracji (w zakresie obowiązującego prawa).

3. Słownik

Lp.	Skrót/Pojęcie	Definicja
1.	**Aktywa**	Sprzęt, oprogramowanie, bazy danych lub urządzenia wspomagające wykorzystywane przez system teleinformatyczny do jego prawidłowego funkcjonowania lub zabezpieczenia go.
2.	**Analiza Ryzyka**	Oszacowanie prawdopodobieństwa oraz skutków zaistnienia zidentyfikowanego ryzyka.
3.	**Audyt**	Niezależna i obiektywna ocena (np. przedsiębiorstwa, procesów, procedur, polityk) zgodności z zadanymi parametrami bądź wskaźnikami (np. przepisy prawa, dobre praktyki, normy).
4.	**Audyt wewnętrzny**	Działalność niezależna i obiektywna, której celem jest przysporzenie wartości i usprawnienie działalności operacyjnej organizacji. Polega na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów: zarządzania ryzykiem, kontroli i ładu organizacyjnego, i przyczyniania się do poprawy ich działania.
5.	**Bezpieczeństwo informacji**	Zachowanie poufności, dostępności, integralności, autentyczności, rozliczalności, niezaprzeczalności i niezawodności informacji.
6.	**Dokumentacja bezpieczeństwa**	Polityka Bezpieczeństwa Informacji wraz z załącznikami oraz raportami, analizami, zestawieniami, rejestrami, planami, programami, itp. powstałymi w cyklu funkcjonowania systemu zarządzania bezpieczeństwem informacji mObywatel.
7.	**Dokumentacja PBI**	Polityka Bezpieczeństwa Informacji wraz z załącznikami; zwrot używany do określenia zestawu dokumentów stanowiących w istocie PBI w kontekście nadzorowania dokumentacji; PBI jest dokumentem (zestawem dokumentów) opisującym rozwiązania organizacyjne i techniczne bezpieczeństwa.
8.	**Incydent Bezpieczeństwa Informacji**	Pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
9.	**Interesariusz**	Osoba bądź jednostka organizacyjna, która wpływa bądź znajduje się pod wpływem określonego zasobu (np. procesu, projektu, procedury, systemu).
10.	**Inspektor ochrony danych (IOD)**	Inspektor ochrony danych w rozumieniu RODO.
11.	**ISO 27001**	Norma międzynarodowa ISO – system zarządzania bezpieczeństwem informacji. Należy rozumieć jako najnowsze wydanie normy ISO/IEC 27001 lub PN-EN ISO/IEC 27001 (szczególnie najnowszą i aktualną wersję polskiej normy PN, a w okresie między

Lp.	Skrót/Pojęcie	Definicja
		ustanowieniem nowej wersji normy ISO/IEC a ustanowieniem jej polskiej wersji normy (PN), należy rozumieć jako najnowszą wersję normy ISO/IEC).
12.	**ITSM**	System do zarządzania usługami IT.
13.	**mObywatel (dawniej mDokumenty)**	Publiczna aplikacja mobilna, o której mowa w art 19e ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, mająca na celu udostępnienie elektronicznej wersji dokumentów (m.in. dowodu osobistego, legitymacji studenckiej/ uczniowskiej, dowodu rejestracyjnego pojazdu) w telefonie komórkowym.
14.	**Monitorowanie**	Proces polegający na weryfikacji parametrów zakładanych z parametrami mierzonymi.
15.	**Monitorowanie realizacji planów naprawczych**	Czynności podejmowane przez audytora wewnętrznego w celu ustalenia stanu realizacji rekomendacji/ zaleceń.
16.	**Niezgodność**	Niespełnienie wymagania (ISO 27000); niespełnienie bądź niewłaściwe realizowanie wymagań dotyczących rozwiązań organizacyjnych i technicznych bezpieczeństwa. Działanie lub rozwiązanie zaburzające lub mogące zaburzyć poprawność przebiegu procesu (czynności, działania systemu, procesu biznesowego, etc).
17.	**Odstępstwo**	Uzgodnione i zatwierdzone działanie lub rozwiązanie organizacyjne lub techniczne różne od zdefiniowanych w PBI. Odstępstwo może być czasowe lub jednorazowe, może być przyznane pojedynczej osobie lub grupie. Nieuzgodnione i niezatwierdzone jest niezgodnością lub incydentem bezpieczeństwa.
18.	**Ryzyko**	Możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów. Ryzyko jest mierzone wpływem (skutkami) i prawdopodobieństwem wystąpienia.
19.	**Security Operations Center (SOC)**	Centrum Bezpieczeństwa Operacyjnego, którego celem jest identyfikacja, monitorowanie oraz poprawa bezpieczeństwa organizacji w cyberprzestrzeni.
20.	**System mObywatel**	System teleinformatyczny, w którego skład wchodzi publiczna aplikacja mobilna mObywatel i mWeryfikator.
21.	**Szacowanie ryzyka**	Całościowy proces: identyfikowania ryzyka, analizy ryzyka i jego oceny.
22.	**SZBI**	System Zarządzania Bezpieczeństwem Informacji
23.	**UODO**	Urząd Ochrony Danych Osobowych. Organ właściwy ds. ochrony danych osobowych na terytorium Polski.
24.	**Urządzenia Mobilne**	Przenośne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią.
25.	**Właściciel Biznesowy (Gestor systemu)**	Osoba, jednostka organizacyjna odpowiedzialna za dane znajdujące się w określonym podległym miejscu (np. w systemie komputerowym).
26.	**Właściciel ryzyka**	Osoba odpowiedzialna za zarządzanie danym ryzykiem w systemie.
27.	**Właściciel systemu**	Minister właściwy ds. informatyzacji.
28.	**Zarządzanie incydentami związanymi z bezpieczeństwem informacji**	Całościowy proces obsługi incydentów związanych z bezpieczeństwem informacji (identyfikowanie, monitorowanie, wykrywanie, raportowanie oraz podejmowanie akcji).
29.	**Zasoby**	Potencjał (np. zasoby ludzkie, sprzętowe, proceduralne, techniczne), który może być użyty do prowadzenia określonej działalności.
30.	**Zdarzenie związane z bezpieczeństwem informacji**	Zdarzenie zaburzające lub mogące zaburzyć poprawność przebiegu procesu obsługi informacji o istotnym znaczeniu.

4. Odpowiedzialność

4.1. Odpowiedzialność w zakresie bezpieczeństwa

Obowiązek przestrzegania postanowień Polityki Bezpieczeństwa Informacji dla systemu mObywatel dotyczy wszystkich interesariuszy systemu. Wszyscy interesariusze mający wpływ na funkcjonowanie systemu, w szczególności ich pracownicy i współpracownicy mają obowiązek zapoznania się z treścią tego dokumentu.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik/współpracownik tych interesariuszy.

Właściciel mObywatel pełni rolę najwyższego kierownictwa w zakresie zarządzania bezpieczeństwem informacji mObywatel i przetwarzanych w nim danych.

Właściciel mObywatel wyraża swoje przywództwo, zaangażowanie i odpowiedzialność w zakresie bezpieczeństwa systemu ustanawiając Politykę Bezpieczeństwa Informacji dla systemu mObywatel i zobowiązując wszystkich interesariuszy do jej przestrzegania i realizacji jej postanowień.

Gestor mObywatel odpowiada za stworzenie i rozwój Systemu Zarządzania Bezpieczeństwem Informacji oraz prowadzi proces ciągłego doskonalenia PBI. Zapewnia również właściwy nadzór nad Polityką Bezpieczeństwa Informacji i związanymi z nią dokumentami, stanowiącymi dokumentację bezpieczeństwa.

4.2. Odpowiedzialność w zakresie kompetencji

Kompetencje rozumiane są jako wiedza, umiejętności i doświadczenie i osiągane są poprzez wykształcenie, szkolenia, staże, udział seminariach, konferencjach, itp.

Właściciel mObywatel oraz każdy z interesariuszy wewnętrznych realizujących zadania na rzecz mObywatel zapewniają odpowiednie kompetencje w zakresie bezpieczeństwa informacji mObywatel swoich pracowników, współpracowników i kontrahentów mających dostęp do danych, do systemu i jego dokumentacji technicznej i eksploatacyjnej oraz realizujących funkcje związane z eksploatacją, utrzymaniem i rozwojem systemu.

Kompetencje w/w osób powinny być adekwatne do zakresów odpowiedzialności zdefiniowanych dla poszczególnych ról w systemie. Niezbędne kompetencje poszczególnych ról w systemie zarządzania bezpieczeństwem informacji mObywatel dotyczą odpowiednio aspektów prawnych i organizacyjnych, technicznych i technologicznych.

Nabywanie, utrzymanie i rozwój kompetencji jest procesem realizowanym w trybie ciągłym przez właściwe komórki organizacyjne każdego z interesariuszy systemu mObywatel. Zakres posiadanych kompetencji podlega okresowej weryfikacji i ocenie.

4.3. Wykaz ról i odpowiedzialności

W zarządzaniu bezpieczeństwem informacji systemem mObywatel istotne znaczenie ma zdefiniowanie ról i ich odpowiedzialności. Dla systemu podstawą do tego są regulacje prawne dotyczące systemu mObywatel oraz zapisy PBI i związanych z nią procedur, które definiują role i ich funkcje w zapewnieniu bezpieczeństwa informacji w rozwoju, eksploatacji i utrzymaniu mObywatel.

Role i ich odpowiedzialności podlegają okresowej weryfikacji przynajmniej jeden raz w roku i w razie potrzeby aktualizacji. Aktualizacja powinna być przeprowadzona również każdorazowo w związku z rozbudową mObywatel o kolejne rejestry i zmianami prawnymi, które mogą definiować zmiany ról.

5. Zgodność prawna

mObywatel działa w ramach określonych przez akty prawne RP. Polityka Bezpieczeństwa Informacji dla systemu mObywatel jest oparta oraz pozostaje w zgodności z obowiązującymi przepisami prawnymi:

- Konstytucja Rzeczypospolitej Polskiej;
- Ustawa z dnia 4 lutego 2011 r. Prawo prywatne międzynarodowe;
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
- Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych;
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
- Rozporządzenie 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);
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r., w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną;
- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej;

- Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi.

6. Interesariusze i użytkownicy mObywatel

W ramach mObywatel można wymienić i scharakteryzować następujące grupy zainteresowanych:

a. właściciel systemu mObywatel,
b. jednostka odpowiedzialna za utrzymanie i eksploatację systemu,
c. jednostka odpowiedzialna za rozwój aplikacji,
d. dostawcy usług/ danych wspomagających mObywatel,
e. dostawca tożsamości,
f. użytkownicy aplikacji.

Właściciel systemu mObywatel

Właścicielem systemu jest minister właściwy ds. informatyzacji. Minister jest podmiotem decyzyjnym w sprawach dotyczących rozwoju oraz utrzymania systemu mObywatel.

Jednostka odpowiedzialna za utrzymanie i eksploatację systemu

Podmiot realizujący zadania z zakresu eksploatacji i utrzymania systemu na rzecz ministra właściwego ds. informatyzacji, zapewniający odpowiedni poziom zabezpieczeń dla powierzonego systemu.

Jednostka odpowiedzialna za rozwój aplikacji

Podmiot realizujący zadania z zakresu wytwarzania i rozwoju systemu na rzecz ministra właściwego ds. informatyzacji, zapewniający odpowiednie zaprojektowanie i zaimplementowanie funkcjonalności oraz rozwiązań ochrony i bezpieczeństwa dla wskazanego systemu na poziomie tworzenia systemu.

Dostawcy usług/ danych wspomagających mObywatel

Podmiotami udostępniającymi usługi/ dane dla mObywatel są podmioty publiczne lub podmioty prywatne świadczące usługi publiczne. Głównymi oczekiwaniami tych podmiotów w zakresie bezpieczeństwa jest zapewnienie stabilności platformy i zaimplementowanych zabezpieczeń oraz zapewnienie atrybutów takich jak niezaprzeczalność, autentyczność, rozliczalność, niezawodność,

poufność i integralność danych.

Dostawca tożsamości

Podmiot odpowiedzialny za rejestrację osób oraz wydawanie im środków identyfikacji elektronicznej w ramach systemu. Wydaje środki identyfikacji na określonych poziomach bezpieczeństwa. Dostawca tożsamości w zakresie wymagań bezpieczeństwa odpowiedzialny jest za zapewnienie atrybutów niezaprzeczalności, autentyczności, rozliczalności, niezawodności, poufności i integralności danych.

Użytkownicy aplikacji

Podmioty korzystające z usług można podzielić na grupy:

- osoby fizyczne (obywatele),
- osoby prawne (przedsiębiorstwa oraz instytucje) – jeżeli nie jest wymagane okazanie dowodu osobistego bądź paszportu,
- podmioty publiczne (np. urzędy, gminy, szpitale, szkoły itp.) – z zastrzeżeniem, że dowód osobisty bądź paszport nie jest wymagany.

Oczekiwaniami tych podmiotów jest zapewnienie atrybutów niezaprzeczalności, autentyczności, rozliczalności, niezawodności, poufności i integralności danych.

7. Zapewnienie bezpieczeństwa informacji

Proces zarządzania bezpieczeństwem informacji jest działaniem realizowanym w sposób ciągły, w oparciu o podejście systemowe zapewniające w sposób uniwersalny adekwatność stosowanych środków ochrony informacji. Wszystkie czynności realizowane w tym procesie podlegają dokumentowaniu oraz cyklicznemu przeglądowi oraz są na bieżąco monitorowane. Zapewnienie ochrony informacji jest realizowane w wielu płaszczyznach jednocześnie zarówno w zakresie organizacyjnym jak i technicznym.

Wszyscy Interesariusze wewnętrzni systemu mObywatel wnoszą wkład w zapewnienie jego bezpieczeństwa w zakresie informacji (danych), na poziomie nie mniejszym niż w stanowią to polityka bezpieczeństwa informacji wraz z procedurami czy umowy zawierane pomiędzy podmiotami.

Najwyższe kierownictwo - minister właściwy ds. informatyzacji oświadcza, że będzie dbał o zapewnienie wysokiego poziomu bezpieczeństwa przetwarzania informacji w systemie mObywatel

w oparciu o obowiązujące przepisy prawa, odpowiednie normy, jak również w oparciu o dobre praktyki z dziedziny bezpieczeństwa informacji.

Wszelkie działania operacyjne w zakresie zarządzania systemem bezpieczeństwa informacji pozostają w zakresie odpowiedzialności Gestora systemu mObywatel.

7.1. Aktywa systemu

Aktywa systemu teleinformatycznego to informacje, osoby, usługi, oprogramowanie, dane i sprzęt, a także inne elementy mające wpływ na bezpieczeństwo informacji. Proces zarządzania aktywami realizowany jest w celu wyeliminowania zagrożeń, czyli niepożądanych zdarzeń, mogących mieć wpływ na informacje.

System mObywatel korzysta z wielu źródeł danych – realizuje funkcje i procesy biznesowe wykorzystując dane zawarte w poszczególnych rejestrach państwowych. W tym zakresie aktywa systemu związane z bezpieczeństwem informacji oraz środkami przetwarzania informacji są zidentyfikowane oraz jest sporządzona i na bieżąco aktualizowana ich ewidencja (zadanie realizuje gestor danego systemu/rejestru). W ramach aktywów ewidencjonowaniu podlegają procesy biznesowe, repozytoria danych oraz pozostałe zasoby (np. zasoby ludzkie czy sprzęt).

7.2. Zarządzanie ryzykiem

Poprzez zarządzanie ryzykiem rozumie się proces, którego zadaniem jest określenie zagrożeń w poddawanym ocenie obszarze oraz ich minimalizacja. Polityka zarzadzania ryzykiem opiera się na metodyce zaproponowanej przez organizację ISO opisanej w dokumencie PN-ISO/IEC 27005. Celem w przypadku zapewnienia bezpieczeństwa informacji jest zachowanie, co najmniej: poufności, integralności oraz dostępności informacji.

Proces zarządzania ryzykiem wiąże się ze stosowaniem określonych reguł we wszystkich obszarach i czynnościach, które mogą być zagrożone wystąpieniem określonych słabości (podatności). Działania zmierzające do obsługi danego ryzyka powinny być prowadzone cyklicznie (np. systematyczna ocena podatności systemu wraz z analizą ryzyka) jak również, jeżeli wymaga tego sytuacja - ad-hoc (np. ocena ryzyka wynikającego ze zmiany w procesie lub zmiany w oprogramowaniu).

Proces zarządzania ryzykiem powinien obejmować następujące części:

1. Identyfikacja kontekstu(otoczenia) – określenie zakresu i granic oraz kryteriów: oceny, skutków i akceptacji ryzyka.
2. Szacowanie ryzyka – identyfikacja, analiza oraz ocena ryzyka.
3. Postępowanie z ryzykiem – modyfikacja, akceptacja, unikanie oraz podzielenie ryzyka.
4. Akceptacja ryzyka – ostateczna akceptacja ryzyka po zastosowaniu wszelkich działań mających na celu dopasowania ryzyka do przyjętych oczekiwań.

Przyjęto, że podczas prowadzenia procesów zarządzania ryzykiem należy stosować techniki jakościowe, oparte na wiedzy eksperckiej dające w dosyć szybkim okresie pogląd całościowy ocenianych aktywów.

Wszystkie czynniki, które mogą mieć wpływ na poziom zidentyfikowanego już ryzyka, jak również powodować nowe zagrożenia, muszą podlegać procesowi monitorowania oraz przeglądu tego obszaru. Monitoringowi podlegają zarówno zabezpieczenia, w wymiarze ich wpływu na redukcję poziomu zagrożenia, czy też redukcję możliwości wykorzystania podatności, jak również same podatności i zagrożenia. Każdy przegląd powinien być udokumentowany i odbywać się, co najmniej 1 raz do roku, jak również ad-hoc w sytuacji zmian wynikających ze specyfiki organizacji czy danego systemu IT. Uprawnieni interesariusze systemu mObywatel powinni mieć dokonane analizy ryzyka (jeżeli ma to odniesienie) w kontekście funkcjonowania systemu mObywatel.

7.3. Postępowanie z incydentami bezpieczeństwa informacji

Każdy pracownik instytucji będącej interesariuszem mObywatel realizujący w nim zadania ma obowiązek dbać o bezpieczeństwo informacji w systemie zgodnie z polityką bezpieczeństwa informacji, oraz reagować na zdarzenia, które mogą wskazywać na wystąpienie incydentu bezpieczeństwa informacji i informować o zdiagnozowanych słabościach systemu.

Zdarzenia, które wiążą się lub mogą wiązać się z naruszeniem bezpieczeństwa informacji to, m.in. naruszenie dowolnego atrybutu bezpieczeństwa systemu (m.in.: poufność, integralność, dostępność, autentyczność) w wyniku umyślnych lub nieumyślnych działań, w szczególności:

- dostęp do systemu osoby nieposiadającej upoważnienia do przetwarzania danych;
- włamanie do systemu lub jego dowolnego komponentu,
- połączenie wydzielonej infrastruktury systemu z dowolną siecią zewnętrzną bez zgody właściciela biznesowego systemu,
- nieuprawnione pozyskanie informacji,
- udostępnienie danych z systemu osobom nieuprawnionym,

- utrata aktywu/zasobu systemu (komputer przenośny, pendrive, dysk, płyta CD z danymi, telefon, dokument, itp.),
- destrukcja danych i oprogramowania systemu,
- próba sabotażu lub sabotaż systemu skutkujący niedostępnością,
- piractwo, kradzież oprogramowania systemu lub oprogramowania wspomagającego (np. licencjonowane oprogramowanie bazy danych),
- oszustwo i fałszerstwo danych systemu,
- szpiegostwo dotyczące danych zawartych w systemie oraz danych dotyczących systemu,
- ujawnienie lub podejrzenie ujawnienia osobom trzecim haseł dostępowych do dowolnych komponentów systemu,
- długotrwała niedostępność systemu lub jego dowolnego komponentu,
- wykrycie szkodliwego oprogramowania w dowolnym komponencie systemu, np.:
  wirusy komputerowe, makrowirusy, robaki, konie trojańskie, bomby logiczne, rootkity, programy szpiegujące, programy reklamowe, keyloggery.

7.4. Zgłaszanie incydentów

Uprawniony interesariusz lub każdy z użytkowników systemu ma obowiązek zgłosić zdarzenia mogące wskazywać na wystąpienie incydentu w obszarze bezpieczeństwa informacji mObywatel bezpośrednio w systemie ITSM dostępnym pod adresem: https://pomoc.coi.gov.pl lub w przypadku braku takiej możliwości: na adres poczty elektronicznej: service_desk_itsm@coi.gov.pl lub telefonicznie na nr.: (42) 25 35 499.

W treści zgłoszenia przekazuje następujące informacje:

- imię i nazwisko oraz dane kontaktowe,
- stanowisko w systemie,
- miejsce wystąpienia incydentu bezpieczeństwa,
- opis incydentu bezpieczeństwa zawierający informacje:
  - na czym polega incydent i czy dotyczy bezpieczeństwa danych prawnie chronionych (np. danych osobowych, informacji niejawnych, tajemnicy przedsiębiorstwa),
  - jakiego elementu systemu (aplikacji) dotyczy,
  - dotyczące daty i godziny wystąpienia lub wykrycia incydentu,
  - na temat wpływu incydentu na elementy systemu,

  - czy incydent nadal trwa lub czy występuje okresowo w sposób powtarzalny,
- wstępną ocenę realnych lub potencjalnych skutków incydentu bezpieczeństwa (oszacowanie szkód),
- podjęte dotychczas działania.

Jeśli osoba zgłaszająca posiada dodatkowe informacje techniczne w postaci konfiguracji sprzętowej, systemu operacyjnego, adresacji sieciowej urządzeń i innych znanych jej kwestii technicznych - dane te powinny być niezwłocznie przekazane po nawiązaniu kontaktu bezpośrednio do linii wsparcia „bezpieczeństwo" w uzgodnionym bezpiecznym kanale komunikacyjnym, przy czym przekazanie danych inicjuje pracownik linii wsparcia „bezpieczeństwo".

Pracownik service desk może żądać od osoby zgłaszającej incydent bezpieczeństwa informacji uzupełnienia opisu.

Niezależnie, czy w toku dalszych działań zgłoszone zdarzenie zostanie sklasyfikowane jako incydent bezpieczeństwa lub inne zdarzenie - service desk informuje o tym osobę zgłaszającą.

Zabrania się działań mogących spowodować utrudnienia w wyjaśnieniu przyczyn incydentu bezpieczeństwa informacji w tym niszczenia, usuwania, ukrywania, modyfikowania informacji i materiałów zawierających dane związane z przedmiotowym incydentem.

7.5. Incydenty dotyczące naruszenia danych osobowych

Inspektor Ochrony Danych Interesariusza odpowiedziany jest za dokonanie szczegółowej analizy incydentu bezpieczeństwa. W przypadku stwierdzenie dojścia do naruszenia ochrony danych osobowych, od momentu stwierdzenia zobowiązany jest w ciągu 72 godzin do zgłoszenia naruszenia ochrony danych do Urzędu Ochrony Danych Osobowych. Zgłoszenie powinno odbyć się przez dedykowany portal udostępniony przez Urząd Ochrony Danych Osobowych w zgodzie z wytycznymi przepisów prawa, ustawy o ochronie danych osobowych.

7.6. Nadzorowanie odstępstw, niezgodności i działań korygujących

Minister właściwy ds. informatyzacji, umocowany przez niego Gestor systemu lub inny pracownik urzędu właściwego ds. informatyzacji odpowiedzialny jest za akceptację odstępstwa.

Osoby (role) wnioskujące o odstępstwa zobowiązane są do podjęcia odpowiednich działań w formie pisemnej, określenia celu, powodu i propozycji postępowania alternatywnego w ramach odstępstwa oraz określenie jego wpływu na bezpieczeństwo informacji oraz system. Gestor nadzoruje

procesowanie odstępstw, niezgodności i działań korygujących, a także zapewnia podejmowanie skutecznych działań korygujących.

Zapewnienie właściwego nadzorowania i procesowania odstępstw, niezgodności i działań korygujących jest kluczowe dla zapewnienia wysokiego poziomu bezpieczeństwa systemu poprzez zapobieganie wykonywania nieuzasadnionych zmian technicznych bądź architektonicznych w systemie oraz wprowadzanie możliwych rozwiązań korygujących eliminujących przyczyny niezgodności w celu zapobiegania ich powtórnego występowania.

Wszelkie informacje dotyczące odstępstw, niezgodności i działań korygujących podlegają udokumentowaniu.

7.7. Monitoring i nadzór

Przegląd zarządzania

Ocena skuteczności wdrożonych zasad zapewniających bezpieczeństwo informacji jest kluczowym elementem systemu zarządzania bezpieczeństwem informacji. Ocena dokonywana jest cyklicznie, podczas przeglądu zarządzania gdzie analizowane są takie elementy jak: wyniki audytów systemu, skuteczność zastosowanych zabezpieczeń, zarządzanie incydentami bezpieczeństwa, realizację celów bezpieczeństwa informacji, działania korygujących.

Audyt wewnętrzny

Audyt wewnętrzny służy potwierdzeniu zgodności systemu mObywatel z wymaganiami dotyczącymi bezpieczeństwa informacji, zarówno w kontekście przepisów prawa stanowionego jak i innych regulacji normatywnych czy wewnętrznych. Jest mechanizmem niezależnej oceny, weryfikującym poziom świadomości i kompetencji użytkowników. Audyt wewnętrzny jest procesem systematycznym - cyklicznie powtarzalnym, który musi być przeprowadzony co najmniej 1 raz do roku.