ZARZĄDZENIE NR 60/2022
WÓJTA GMINY GNIEZNO

z dnia 13 lipca 2022 r.

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Gniezno

Na podstawie § 20 ust. 1 i 2 rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, niniejszym zarządza się co następuje:

§ 1. Wdraża się w Urzędzie Gminy Gniezno System Zarządzania Bezpieczeństwem Informacji stanowiący załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Urzędu Gminy Gniezno do stosowania postanowień wynikających z Systemu Zarządzania Bezpieczeństwem Informacji.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Gniezno

Maria Suplicka

Załącznik do zarządzenia Nr 60/2022
Wójta Gminy Gniezno
z dnia 13 lipca 2022 r.

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

URZĄD GMINY GNIEZNO

AL. REYMONTA 9/11, 62-200 GNIEZNO

`

SPIS TREŚCI

ROZDZIAŁ I

Postanowienia ogólne……4

ROZDZIAŁ II

Polityka Bezpieczeństwa Informacji – PBI……...6

ROZDZIAŁ III

Tabela zmian Systemu Zarządzania Bezpieczeństwa Informacji (SZBI)……...12

ROZDZIAŁ I

Postanowienia ogólne

§ 1

Podstawa prawna

Niniejszy System Zarządzania Bezpieczeństwem Informacji został sporządzony na podstawie międzynarodowych standardów bezpieczeństwa informacji i jest zgodny z obowiązującymi normami prawnymi, w szczególności z:

1. Konstytucją Rzeczypospolitej Polskiej (Dz.U. Nr 78, poz. 483), zwaną dalej „Konstytucja RP”;
2. Rozporządzeniem 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) (Dz. Urz. UE L 119 z 2016 r.), zwanym dalej: „RODO”;
3. Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r.poz. 1781), zwana dalej: „ustawa uodo”;
4. Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742), zwana dalej: „ustawa o informacjach niejawnych”;
5. Ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2020 r. poz. 1913), zwana dalej: „ustawą znk”;
6. Ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r. poz. 2176), zwana dalej: „dostęp do informacji publicznej”;
7. Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 poz. 1369), zwana dalej: „ustawa o cyberbezpieczeństwie”;
8. Rozporządzeniem 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 (Dz.U. z 2017 r. poz. 2247), zwane dalej: „rozporządzenie KRI”;
9. Normą ISO/IEC 27001, zwana dalej: „norma ISO”.

§ 2

Cel SZBI

Celem wdrożonego Systemu Zarządzania Bezpieczeństwa Informacji w Urzędzie Gminy Gniezno w skrócie „SZBI" jest zapewnienie zachowania poufności, integralności i dostępności informacji w wyniku stosowania procesu zarządzania ryzykiem, a także:

1. Zagwarantowania właściwej ochrony informacji, w tym odpowiedniego poziomu bezpieczeństwa informacji bez względu na jakim nośniku została ona zapisana;
2. Zapewnienia ciągłości procesów przetwarzania informacji;
3. Ograniczenia występowania zagrożeń dla bezpieczeństwa informacji;
4. Zapewnienia właściwego funkcjonowania wszystkich systemów informatycznych;
5. Właściwego reagowania na incydenty bezpieczeństwa informacji.

§ 3

Skład SZBI

System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Gniezno zapewnia kompleksową regulację w zakresie bezpieczeństwa informacji, w której skład wchodzą następujące dokumenty:

1. **Polityka Ochrony Danych Osobowych** wprowadzona Zarządzeniem nr 88/2019 z dnia 31.12.2019 r.
2. **Plan Ochrony Informacji Niejawnych** wprowadzona Zarządzeniem nr 74/2021 z dnia 28 października 2021 r
3. **Polityka Bezpieczeństwa Informacji** wprowadzona w rozdziale II niniejszego dokumentu jakim jest System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Gniezno.

§ 4

Zasady postępowania z określonymi informacjami

W Urzędzie Gminy Gniezno poszczególne informacje są chronione na podstawie przepisów prawa. W oparciu o wymagania prawne nakładane na ochronę aktywów informacyjnych dokonano podziału na właściwe klasy chronionych informacji. Najważniejsze grupy informacji objęte wymaganiami to:

1. Dane osobowe.
2. Informacje niejawne.
3. Informacje objęte tajemnicą skarbową.
4. Informacje publiczne.

5. Informacje finansowe.
6. Informacje stanowiące tajemnice przedsiębiorstwa, w szczególności informacje występujące w umowach zawartych z dostawcami usług zewnętrznych.

ROZDZIAŁ II

Polityka Bezpieczeństwa Informacji - PBI

§ 5

Podejście do bezpieczeństwa informacji

Podejście do bezpieczeństwa informacji w Urzędzie Gminy Gniezno zostało oparte na kluczowych regułach dla funkcjonowania organizacji w zakresie zarządzania szeroko pojętym aktywem jakim jest informacja.

1. **Reguła poufności informacji** - zapewniająca, że informacja jest udostępniana jedynie osobom upoważnionym do jej przetwarzania.
2. **Reguła integralności informacji** - zapewniająca zupełną dokładność i kompletność informacji oraz metod jakimi jest ona przetwarzana.
3. **Reguła dostępności informacji** - zapewniająca, że osoby upoważnione do przetwarzania posiadają dostęp do oznaczonej informacji wówczas, gdy istnieje taka potrzeba.

§ 6

Bezpieczeństwo organizacyjne

1. Dostęp do aktywów oraz zasobów informacyjnych w Urzędzie Gminy Gniezno jest realizowany za pomocą zatwierdzonych sposobów postępowania oraz mechanizmów kontrolnych w obszarach fizycznego dostępu do informacji oraz danych przetwarzanych w systemach informatycznych zastosowanych w Urzędzie.
2. Procedura bezpiecznego postępowania z kluczami dostępu do pomieszczeń w Urzędzie Gminy Gniezno stanowi załącznik nr 1 do Systemu Zarządzania Bezpieczeństwem Informacji.

§ 7

Odpowiedzialność za aktywa

1. Odpowiedzialność za aktywa w postaci informacji oraz urządzeń i kluczy dostępu spoczywa na każdym z zobowiązanych uczestników SZBI. Ponadto odpowiedzialność za bezpieczeństwo informacji spoczywa na każdym uczestniczącym w procesie przetwarzania informacji na mocy udzielonego upoważnienia do przetwarzania danych osobowych oraz regulacji wynikających z przetwarzania informacji niejawnych w Urzędzie Gminy Gniezno.
2. Oświadczenie o zapoznaniu pracownika z Systemem Zarządzania Bezpieczeństwem Informacji stanowi załącznik nr 2 do Systemu Zarządzania Bezpieczeństwem Informacji.

§ 8

Analiza ryzyka bezpieczeństwa informacji

Szacowanie ryzyka dla bezpieczeństwa informacji przetwarzanych w Urzędzie Gminy Gniezno zostało określone w załączniku nr 3 do Systemu Zarządzania Bezpieczeństwem Informacji. Analiza ryzyka dokonywana jest przy wykorzystaniu ryzyk określonych w polityce ochrony danych osobowych z uwzględnieniem ryzyk dla bezpieczeństwa informacji wskazanych w powyżej wymienionym załączniku.

§ 9

Organizacja bezpieczeństwa informacji przy pracy z wykorzystaniem urządzeń mobilnych

Wykorzystanie urządzeń mobilnych w Urzędzie Gminy Gniezno kompleksowo reguluje procedura w postaci regulaminu korzystania z urządzeń mobilnych stanowiącego załącznik nr 4 do Systemu Zarządzania Bezpieczeństwem Informacji.

§ 10

Bezpieczeństwo określonych informacji

1. Dane osobowe – w przypadku informacji stanowiących dane osobowe należy każdorazowo odnieść się do zapisów wdrożonej polityki ochrony danych osobowych oraz procedur z niej wynikających.
2. Informacje niejawne – stanowią wszelkie informacje, dla których przetwarzania ustanowiono plan ochrony informacji niejawnych.

3. Informacje publiczne – informacje podlegające ochronie do momentu ich upublicznienia przez Urząd Gminy Gniezno. Dostęp do informacji publicznych pozostaje ograniczony w zakresie prawnie chronionych informacji, których ochrona wynika bezpośrednio z przepisów obowiązującego prawa. Upublicznieniu mogą podlegać jedynie informacje, które zostały podane uprzedniej analizie udostępnienia. Informacje w postaci potencjalnych podatności, incydentów, zagrożeń dla cyberbezpieczeństwa oraz ryzyku wystąpienia incydentów nie podlegają udostępnieniu w trybie ustawy o dostępie publicznym zgodnie z art. 37 ust. 1 ustawy o cyberbezpieczeństwie.
4. Informacje objęte tajemnicą skarbową – informacje chronione na mocy art. 293 ustawy z dnia 29 sierpnia 1993 r. Ordynacja podatkowa.
5. Informacje finansowe – informacje chronione na mocy art. 99 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.
6. Informacje stanowiące tajemnice przedsiębiorstwa – informacje należy przetwarzać zgodnie z przepisami o zwalczaniu nieuczciwej konkurencji, przepisami o dostępie do informacji publicznej, warunkami umowy lub porozumienia, w szczególności wymaganiami określonymi w zapisach umownych dotyczących zachowania poufności.

§ 11

Bezpieczeństwo w relacji z dostawcami usług zewnętrznych

Umowy zawierane z firmami świadczącymi usługi zewnętrzne, powinny zawierać zapisy odnośnie kwestii bezpieczeństwa informacji z szczególnym uwzględnieniem ochrony danych osobowych w przypadku niezbędności ich przetwarzania przy realizacji umowy.

1. Zapisy umowy powierzenia wynikają wprost z polityki ochrony danych osobowych przyjętej w Urzędzie Gminy Gniezno.
2. Należy stosować zapisy zobowiązujące do zachowania w poufności informacji ujawnionych w ramach realizacji poszczególnych umów.

§ 12

Zarządzanie incydentami bezpieczeństwa informacji

Wystąpienie incydentu informatycznego spowodowanego ingerencją podmiotu zewnętrznego w systemy mające zastosowanie w Urzędzie Gminy Gniezno powoduje konieczność podjęcia zgłoszenia do krajowego zespołu reagowania na incydenty bezpieczeństwa komputerowego

pod adresem e-mail: cert@cert.pl przy pomocy formularza online dostępnego na stronie internetowej: https://incydent.cert.pl

1. Osobą odpowiedzialną za dokonanie zgłoszenia jest Informatyk wyznaczony w Urzędzie Gminy Gniezno.
2. Zgłoszenie należy dokonać w terminie nie późniejszym, aniżeli w ciągu 24 godzin od momentu wykrycia incydentu.
3. Zgłoszenie incydentu bezpieczeństwa informatycznego do CERT Polska, nie zwalnia z obowiązku zgłoszenia naruszeń wynikających z wdrożonej w Urzędzie Gminy Gniezno dokumentacji z zakresu ochrony danych osobowych czy informacji niejawnych.

§ 13

Plan ciągłości działania

Celem planu ciągłości działania jest minimalizacja zakłóceń w trakcie realizacji działalności przez Urząd Gminy Gniezno w związku z sytuacją ingerującą bezpośrednio na prawidłowość pracy jednostki.

1. Zaistnienie dysfunkcji systemu informatycznego uniemożliwiającego dalszą pracę w systemie powoduje odniesienie się do zdefiniowanych działań koniecznych do podjęcia w danym przypadku, określonych w poniższej tabeli:

Lp.	Funkcja	Opis działań	Zasoby
1.	Weryfikacja zasadności zgłoszenia od użytkownika.	Weryfikacja, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.	- dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie.
2.	Ustalenie źródła awarii.	Ustalenie, co jest przyczyną awarii: - przerwa w zasilaniu prądem, - brak połączenia z siecią Internet, - wadliwe działanie sprzętu, - wadliwe działanie aplikacji, - wadliwe działanie systemu, na którym uruchomiona jest aplikacja.	- dostęp do serwerowni oraz do sprzętu, który uległ awarii, - kontakt z osobą, która może w porze nocnej pobrać klucze od ośrodka, - w przypadku zablokowania zamka wezwać ślusarza, - w przypadku awarii zasilania elektrycznego wezwać elektryka.
3.	Określenie skali awarii.	Ustalenie, czy awaria powoduje zatrzymanie pracy: - jednego pomieszczenia pracy lub działu (od 1 do 10 osób); - kilku wydziałów; - całego budynku jednostki.	- kontakt z kluczowymi pracownikami działów oraz listę z numerami telefonów.
4.	Ustalenie czy wznawianie usługi może odbywać się w dotychczasowej	Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.	- możliwość uruchomienia dowolnych usług w lokalizacji, - infrastrukturę sieciową, zasilanie prądem.

	lokalizacji.		
5.	Zakup niezbędnych elementów wyposażenia, dokonanie naprawy bądź wymiany urządzeń, uruchomienie aplikacji.	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer).	- środki na zakup elementów niezbędnych do ponownego uruchomienia systemu.
6.	Weryfikacja możliwości przeniesienia aplikacji na inny serwer.	Sprawdzenie, czy aplikacja może być uruchomiona na którymś z działających poprawnie w jednostce serwerów.	- dostęp do alternatywnego serwer.
7.	Przygotowanie serwera zastępczego.	Serwerem zastępczym można ustanowić np. komputer typu stacja robocza, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.	- maszynę dowolnego typu, która w podstawowym zakresie pozwoli na uruchomienie podstawowych usług.
8.	Podjęcie decyzji o terminie odtworzenia maszyny.	W razie konieczności należy skontaktować się z kluczowymi pracownikami wydziałów.	- kontakt z kluczowymi pracownikami wydziałów Urzędu Gminy Gniezno.
9.	Przywrócenie funkcjonowania systemu.	Usunięcie przyczyny nieprawidłowego działania systemu. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych.	- dostęp do najbardziej aktualnej wersji aplikacji, - dostęp do aktualnej bazy danych.
10.	Sprawdzenie systemu bądź aplikacji.	Przeniesienie bądź uruchomienie należy potwierdzić weryfikacją prawidłowego funkcjonowania systemów zainstalowanych na serwerze bądź aplikacji.	- dostęp do serwera i stacji roboczych.
11.	Uruchomienie usługi w systemie informatycznym Urzędu Gminy Gniezno.	Uruchomienie usługi należy zakomunikować zainteresowanym użytkownikom jednostki.	- kontakt z kluczowymi pracownikami wydziałów Urzędu Gminy Gniezno.

2. Osobą odpowiedzialną za funkcjonowanie planu ciągłości działania pozostaje Sekretarz przy udziale Informatyka.
3. Test planu ciągłości działania polega na wykonaniu symulacji wyłączenia serwera danej aplikacji, uniemożliwiając tym samym możliwość wykonywania usług. Rezultatem oczekiwanym testu jest możliwość wznowienia działania usługi na nowej maszynie. Symulacji należy dokonać z udokumentowaniem czynności w protokole, którego wzór stanowi załącznik nr 5 do niniejszego Systemu Zarządzania Bezpieczeństwem Informacji.
4. Zakłócenia działalności mogące wystąpić w wyniku klęski żywiołowej na wypadek, której zostało ustanowione postępowanie w rozdziale 6 wdrożonej polityki ochrony danych osobowych w Urzędzie Gminy Gniezno.

ROZDZIAŁ III

Tabela zmian Systemu Zarządzania Bezpieczeństwa Informacji (SZBI)

Lp.	Paragraf/punkt	Data wprowadzonej zmiany	Opis dokonanej zmiany w SZBI

Załącznik nr 1 do SZBI

Procedura
postępowania z kluczami

1. Klucze do pomieszczeń przechowywane są w Biurze Obsługi Klienta (pomieszczenie przechowywania kluczy) w zamykanej na klucz szafie (miejsce przechowywania kluczy). Za zabezpieczenie miejsca przechowywania kluczy odpowiada wyznaczony pracownik Referatu Organizacyjnego, Spraw Obywatelskich i Promocji, który prowadzi rejestr wszystkich posiadanych kluczy oraz przyjmuje i wydaje klucze. Od momentu pobrania kluczy do momentu ich zdania, na pracownikach pomieszczeń, w których usytuowane są ich miejsca pracy, spoczywa odpowiedzialność za ochronę pomieszczeń oraz mienie znajdujące się w tych pomieszczeniach w godzinach pracy Urzędu.
2. Z uwagi na publiczny charakter Urzędu w godzinach otwarcia nie obowiązuje system przepustek ani też inny system, który określałby uprawnienia do wejścia, przebywania i wyjścia z Urzędu.
3. Pracownikom urzędu zabrania się:
    1) dorabiania dodatkowych kluczy do pomieszczeń i budynku Urzędu Gminy Gniezno,
    2) udostępniania kluczy osobom trzecim,
    3) pozostawiania kluczy bez nadzoru,
    4) zabierania kluczy do domu.
4. W przypadku zagubienia klucza pracownik zobowiązany jest powiadomić Sekretarza, który decyduje o konieczności wyrobienia duplikatu.
5. Zamówienie duplikatu klucza zajmuje się Wydział Organizacyjny.
6. Po ustaniu zatrudnienia lub współpracy pracownik lub współpracownik zobowiązany jest do zwrotu wszystkich posiadanych kluczy do Sekretarza, który następnie przekazuje je do Wydziału Organizacyjnego.
7. Do obowiązków wszystkich pracowników Urzędu należy w szczególności:
    1) Po zakończeniu dnia pracy, pracownicy urzędu zobowiązani są do uporządkowania swoich stanowisk pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, w szczególności polegających na:

a. zabezpieczeniu dokumentacji - polegającym na trwałym zniszczeniu w niszczarce lub schowanie do zamykanych na klucz pomieszczeń i szaf wszelkich wykonanych wydruków dokumentów zawierających dane osobowe,
b. schować wszelkie akta zawierające dane osobowe,
c. klucze do szaf, biurek itp.- umieścić w przyjętym zabezpieczonym miejscu,
d. zabezpieczyć komputery, urządzenia mobilne,
e. klucze do pomieszczeń służbowych należy zostawić wyznaczonemu pracownikowi Referatu Organizacyjnego, Spraw Obywatelskich i Promocji.

2) W trakcie pracy pracownik zobowiązany jest do:
   a. zwracanie uwagi na zachowanie osób wchodzących i wychodzących z Urzędu,
   b. natychmiastowe reagowanie na wejście do budynku osób będących pod wpływem alkoholu lub innych środków odurzających,
   c. natychmiastowe reagowanie na próby niszczenia, wynoszenia lub wywożenia mienia z budynku Urzędu,
   d. natychmiastowe reagowanie na próby wnoszenia lub wywożenia przedmiotów niebezpiecznych, materiałów lub substancji budzących podejrzenie,
   e. natychmiastowe reagowanie poprzez powiadomienie odpowiednich służb, pracowników o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia a także utraty lub zniszczenia mienia.

8. Do zadań pracowników obsługi wykonujących usługi sprzątające w budynku pracy należy:
   1) w szczególności nie udostępniania powierzonego klucza osobom trzecim.
   2) w przypadku awarii, zabezpieczanie miejsca awarii, zawiadomienie osoby upoważnionej, a w razie zaistnienia potrzeby wezwanie także odpowiednich służb.

Załącznik nr 2 do SZBI

…… dnia, ……..

OŚWIADCZENIE
o zapoznaniu z Systemem Zarządzania Bezpieczeństwem Informacji

Niniejszym oświadczam, iż zostałem zapoznany z wdrożonym Systemem Zarządzania Bezpieczeństwem Informacji oraz zobowiązuję się do przestrzegania postanowień w nim zawartych.

……
podpis

Załącznik nr 3 do SZBI

SZACOWANIE RYZYKA
dla bezpieczeństwa informacji

Podatności mogące prowadzić do wystąpienia ryzyk dla bezpieczeństwa informacji w Urzędzie Gminy Gniezno (1 – niskie, 2 – średnie, 3 – wysokie):

1. Wprowadzenie kodu złośliwego – sieć LAN

Lp.	Ryzyko	Podatność
1.		Złe umiejscowienie w systemie lub brak aktualizacji bądź brak oprogramowania typu AV.
2.		Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja zapór sieciowych.
3.		Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja oprogramowania typu IPS/IDS.
4.		Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach LAN.

2. Wniknięcie kodu złośliwego – sieć WAN

Lp.	Ryzyko	Podatność
1.		Złe umiejscowienie w systemie lub brak aktualizacji bądź brak oprogramowania typu AV.
2.		Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja zapór sieciowych.
3.		Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja oprogramowania typu IPS/IDS.
4.		Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach WAN.
5.		Nie monitorowanie bieżącego obciążenia serwerów.
6.		Podatność użytkowników systemu na oddziaływanie metod inżynierii społecznej, mającej na celu uzyskania informacji lub wprowadzenia złośliwego kodu.

3. Nieautoryzowany dostęp do informacji

Lp.	Ryzyko-	Podatność
1.		Brak nadzoru nad uprawnieniami użytkowników.
2.		Nadane uprawnienia nieadekwatne do wykonywanych zadań.
3.		Brak wnoszenia zmian uprawnień użytkowników.
4.		Brak kontroli fizycznego dostępu do elementów systemu.

4. Zagrożenie atakiem DDoS lub DoS

Lp.	Ryzyko	Podatność
1.		Brak nadzoru nad ruchem w sieci.
2.		Występowanie błędu oprogramowania.
3.		Wykorzystywanie przestarzałego sprzętu do obsługi systemu.
4.		Brak działań w celu wymiany sprzętu na nowocześniejszy.
5.		Brak monitorowania obciążenia serwerów.
6.		Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja oprogramowania.
7.		Brak lub niewłaściwe umiejscowienie w topologii sieci bądź zła konfiguracja zapór sieciowych.

5. Podsłuch/przechwyt danych

Lp.	Ryzyko	Podatność
1.		Brak nadzoru nad ruchem w sieci.
2.		Brak szyfrowania w łączach WAN.
3.		Podsłuch informacji w sieci wewnętrznej LAN.
4.		Pozyskiwanie informacji z nośników danych wycofanych z użycia.

6. Służbowe telefony komórkowe

Lp.	Ryzyko	Podatność
1.		Zagubienie telefonu komórkowego.
2.		Kradzież telefonu komórkowego.
3.		Zniszczenie telefonu komórkowego.
4.		Pozyskanie poufnych informacji wyświetlanych na ekranie.

5.		Pobranie aplikacji zawierającej złośliwy kod.
6.		Korzystanie z niezabezpieczonej sieci WIFI.

7. Rozmowy telefoniczne

Lp.	Ryzyko	Podatność
1.		Przekazanie informacji poufnej w trakcie rozmowy telefonicznej.
2.		Dokonanie określonej przez rozmówcę czynności wywołującej szkodę.

8. Kontakt drogą e-mail

Lp.	Ryzyko	Podatność
1.		Dokonanie w treści podejrzanej wiadomości, określonej przez adresata czynności.

Zabezpieczenia możliwe dla zastosowania w celu minimalizacji ryzyk dla bezpieczeństwa informacji w Urzędzie Gminy Gniezno:

1. Wprowadzenie kodu złośliwego – sieć LAN

Lp.	Działanie zabezpieczające
1.	Blokowanie portów USB na stacjach roboczych.
2.	Nadzór nad niewykorzystywanymi zakończeniami sieci LAN.
3.	Autoryzacja dostępu do serwera.
4.	Zastosowanie oprogramowania klasy AV na stacjach roboczych.
5.	Blokowanie możliwości instalowania oprogramowania przez użytkownika.
6.	Weryfikacja zainstalowanego oprogramowania na stacjach roboczych.

2. Wniknięcie kodu złośliwego – sieć WAN

Lp.	Działanie zabezpieczające
1.	Translacja adresów sieciowych.
2.	Oprogramowanie klasy AV na styku sieci WAN z LAN.
3.	Systemy klasy IDS/IPS.
4.	Zastosowanie serwerów PROXY.
5.	Wykrywanie oraz blokowanie spamu.
6.	Budowanie topologii sieci z uwzględnieniem obszarów bezpiecznych.

3. Nieautoryzowany dostęp do informacji

Lp.	Działanie zabezpieczające
1.	Procedury nadawania i odbierania uprawnień w systemie.
2.	Procedury przeglądania uprawnień w systemach.
3.	Rozpraszanie uprawnień.

4. Zagrożenie atakiem DDoS lub DoS

Lp.	Działanie zabezpieczające
1.	Stosowanie techniki rozpraszania danych.
2.	Przejście na statyczne wersje serwisu po wykryciu ataku typu DDoS/DoS.
3.	Blokowanie ruchu sieciowego z określonych adresów IP.
4.	Monitorowanie ruchu w sieci.

5. Podsłuch/przechwyt danych

Lp.	Działanie zabezpieczające
1.	Stosowanie urządzeń o obniżonej emisji ujawniającej.
2.	Prowadzenie okablowania sieciowego w zamkniętych kanałach.
3.	Nadzór nad niewykorzystywanymi zakończeniami sieci LAN.
4.	Stosowanie strefowania.

6. Służbowe telefony komórkowe

Lp.	Działanie zabezpieczające
1.	Stosowanie blokady telefonu przy pomocy hasła.
2.	Stosowanie blokady telefonu przy pomocy hasła oraz
3.	Tworzenie kopii zapasowych.
4.	Czasowa blokada wyświetlacza.
5.	Pobieranie zweryfikowanych aplikacji z zaufanych źródeł.
6.	Korzystanie z zweryfikowanych, zaufanych sieci WIFI.

7. Rozmowy telefoniczne

Lp.	Działanie zabezpieczające
1.	Przeprowadzanie testów socjotechnicznych oraz szkoleń pracowników.

8. Kontakt drogą e-mail

Lp.	Działanie zabezpieczające
1.	Przeprowadzanie testów socjotechnicznych oraz szkoleń pracowników.

Załącznik nr 4 do SZBI

REGULAMIN
korzystania ze służbowych urządzeń mobilnych

I. Wprowadzenie

1. Niniejszy regulamin określa zasady korzystania ze służbowego sprzętu i obowiązuje każdego użytkownika sprzętu bez wyjątku.
2. W Regulaminie pod określeniem „użytkownik" należy rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak i współpracowników, na stale wykonujących zadania w ramach umów cywilnoprawnych, które korzystają ze służbowego sprzętu elektronicznego.
3. Przez „pracodawcę" należy rozumieć zarówno pracodawcę, jak i zlecającego usługi. Pracodawca jest podmiotem, który powierza użytkownikowi sprzęt służbowy.
4. Użytkownik ma obowiązek wykorzystywać do realizowania powierzonych mu zadań służbowe urządzenia mobilne powierzone przez pracodawcę, tzn. telefon, smartfon, laptop, tablet lub inne urządzenia elektroniczne.
5. Korzystanie z prywatnych urządzeń jest dopuszczalne tylko i wyłączenie po otrzymaniu wcześniejszej, udokumentowanej zgody pracodawcy.
6. Właściwe użytkowanie służbowych urządzeń mobilnych ma duże znaczenie dla bezpieczeństwa zasobów informacyjnych w organizacji.
7. Złamanie zasad określonych w Regulaminie lub niedostosowanie się do postanowień niniejszego Regulaminu może stanowić naruszenie obowiązków pracowniczych. W przypadku osób realizujących zadania w oparciu o umowy cywilnoprawne postępowanie niezgodnie z niniejszym Regulaminem może oznaczać wykonanie zadania niezgodnie z przedmiotem umowy i z wymaganą przez pracodawcę starannością i zawodowym profesjonalizmem i skutkować rozwiązaniem umowy, a także przewidzianymi w umowie karami umownymi.

II. Warunki korzystania z urządzeń mobilnych

1. Urządzenie mobilne powierzone przez pracodawcę jest przeznaczone do realizowania przez użytkownika powierzonych mu zadań i w takim celu należy je wykorzystywać.

2. Niedozwolone jest wykorzystywanie służbowych urządzeń mobilnych do prywatnych celów.
3. Użytkownikowi nie wolno pożyczać lub udostępniać powierzonego mu sprzętu innym osobom.
4. Użytkownik odpowiada za zapewnienie ochrony fizycznej powierzonych mu urządzeń mobilnych, gdy korzysta z nich poza siedzibą pracodawcy. W przypadku jego utraty lub zgubienia, użytkownik niezwłocznie zgłasza ten fakt pracodawcy. Następnie należy podjąć działania minimalizujące ryzyko negatywnych skutków zdarzenia, zgodnie z Procedurą postępowania w przypadku naruszenia ochrony danych osobowych oraz incydentu dla naruszenia bezpieczeństwa informacji.
5. Pracodawca powierza użytkownikowi sprzęt z zainstalowanym oprogramowaniem, które jest niezbędne do realizowania jego zadań. Użytkownik jest zobowiązany korzystać tylko i wyłączenie z oprogramowania zainstalowanego i dostarczonego przez pracodawcę. Zabronione jest samodzielne instalowanie oprogramowania, a w przypadku złamania zakazu użytkownik ponosi odpowiedzialność wynikającą zarówno z postanowień licencyjnych tego oprogramowania, jak i ewentualnego nieprawidłowego działania lub naruszenia bezpieczeństwa zasobów informacyjnych pracodawcy.
6. Pracodawca zapewnia na udostępnionych urządzeniach mobilnych zabezpieczenia, jak: program antywirusowy, automatyczne aktualizacje, zapora sieciowa, szyfrowanie, ograniczenie uprawnień. Zabronione jest ingerowanie w zabezpieczenia zainstalowane na urządzeniach.
7. Użytkownik niezwłocznie zgłasza pracodawcy wszelkie problemy techniczne, jak problemy związane z aktualizacją oprogramowania, błędy programu antywirusowego, podejrzane działania oprogramowania, itp.
8. Użytkownik korzystając z urządzeń mobilnych przestrzega zasad ochrony danych osobowych, wynikających z wewnętrznych polityk ochrony danych obowiązujących u pracodawcy.
9. Ze względu na bezpieczeństwo danych przechowywanych w służbowych urządzeniach mobilnych, zakazane jest podłączanie tych urządzeń do publicznych sieci WiFi (np. w hotelach, galeriach handlowych, środkach komunikacji publicznej, lotniskach) oraz sieci WiFi u kontrahentów (w przypadku wizyt służbowych u kontrahentów).

10. Użytkownik jest zobowiązany do zapewnienia poufności danych dostępowych do jego służbowych urządzeń mobilnych i do pracowania tylko i wyłączenie na swoim koncie użytkownika. Zabronione jest posługiwanie się cudzym loginem.
11. W przypadku używania zewnętrznych nośników danych (np. dysk zewnętrzny, CD, pendrive) użytkownik jest zobowiązany wykonać przed otwarciem zawartości urządzenia skanowanie nośnika programem antywirusowym.
12. Przekazywanie informacji poufnych, w tym danych osobowych drogą elektroniczną, wymaga uprzedniego zabezpieczenia hasłem tych informacji. Hasło w takim wypadku powinno zostać przekazane odbiorcy inną drogą komunikacji.
13. Niedozwolone jest podejmowanie pracy na służbowych urządzeniach mobilnych, gdy niezbędny jest dostęp do danych osobowych, w miejscach publicznych i ogólnodostępnych, jak kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
14. Pracując w domu użytkownik musi zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu urządzenia, a także blokowanie go podczas zawieszenia pracy i wylogowanie po zakończeniu pracy.
15. Użytkownik przekazuje służbowe urządzenie mobilne do przeglądu na każde wezwanie wyznaczonego w Urzędzie Informatyka.
16. Służbowe urządzenie mobilne może zostać przekazane innemu użytkownikowi, tylko po uprzednim, skutecznym usunięciu z niego informacji, w tym danych osobowych. Za usunięcie danych na urządzeniach przeznaczonych do wtórnego użytku oraz ich przygotowanie do przekazania innemu użytkownikowi odpowiada wyznaczony w Urzędzie Informatyk.
17. Użytkownik nie jest uprawniony do samodzielnego przekazania urządzenia innemu użytkownikowi.
18. Korzystanie z programów służących do przetwarzania danych osobowych na służbowych urządzeniach mobilnych odbywa się po uwierzytelnieniu użytkownika do tego programu. Konieczność zabezpieczenia aplikacji poprzez dodatkowe hasło dostępu, dotyczy także smartfonów, gdzie może być niezbędne ręczne ustawienie konieczności podania dodatkowego hasła do aplikacji. Wsparcia w zakresie konfiguracji ustawień udziela wyznaczony w Urzędzie Informatyk, jednakże to

użytkownik odpowiada za nadzór, aby na użytkowanych przez niego urządzeniach zostały spełnione wskazane warunki bezpieczeństwa dostępu do aplikacji.

III. Bezpieczeństwo korzystania z Internetu

1. W biurze użytkownik powinien korzystać ze służbowej sieci internetowej.
2. Poza Urzędem użytkownik powinien korzystać z dostępu do Internetu zapewnionego przez pracodawcę w ramach dostarczonych narzędzi służbowych, tzn. modem, router, punkt HotSpot udostępniony ze służbowego urządzenia, itp.
3. Użytkownik informuje pracodawcę, jeżeli do prawidłowego użytkowania służbowych urządzeń mobilnych jest niezbędne udostępnienie mu narzędzi do bezpiecznego łączenia się z Internetem.
4. Zabronione jest korzystanie z publicznych sieci WiFi.
5. Dopuszczalne jest korzystanie z domowej sieci WiFi, jednakże pod wskazanymi warunkami:
   a) Korzystanie z Internetu wymaga uwierzytelnienia, np. poprzez hasło,
   b) Hasło dostępu spełnia warunki, jakie stawia hasłom wewnętrzna polityka ochrony danych u pracodawcy.
   c) Login do panelu administracyjnego routera został zmieniony z domyślnego na własny.
   d) Dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej.
   e) Został zmieniony domyślny adres routera (najczęściej 192.168.1.1.) na inny.
6. Porad i wsparcia w zakresie konfiguracji sieci domowej, w tym jej zabezpieczenia na potrzeby pracy zdalnej udziela wyznaczony w Urzędzie Informatyk.

Załącznik nr 5 do SZBI

…… dnia,……

PROTOKÓŁ
z testu planu ciągłości działania

Nr ……. z dnia ……..… .

1. Termin dokonanego testu: ……
2. Osoba odpowiedzialna za przeprowadzenie testu: ……..
3. Osoby uczestniczące w przeprowadzanym teście: ……..
4. Scenariusz testu planu ciągłości działania: ……..
5. Wynik przeprowadzonego testu: ……..
6. Osoba zatwierdzająca wynik przeprowadzonego testu: ……..

……

podpis