Załącznik Nr 02c
do Polityki Ochrony Danych Osobowych
w Miejskim Ośrodku Pomocy Społecznej
w Częstochowie

Arkusz analizy ryzyka

P - Prawdopodobieństwo incydentu (skala od 1 do 3), S - Skutki wystąpienia incydentu (skala od 1 do 3), R - Ryzyko wystąpienia incydentu (skala od 1 do 9), Formuła: R=P*S

Zagrożenie	Opis zagrożenia	P	S	R	Zabezpieczenie
Phishing, cybersquatting (podrabianie stron)	• Mail z prośbą o zalogowanie się (pod pretekstem weryfikacji danych lub informowanie o próbie włamania na konto) do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła • Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie do www.rnbank.pl	1	2	2	**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • blokada dostępu do określonych stron
Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery)	2	1	2	**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • blokada dostępu do określonych stron • poziomy uprawnień w systemach operacyjnych i domenach
Podrzucone nośniki danych	Atakujący pozostawia specjalnie przygotowany pendrive z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu przypadkach z CIEKAWOŚCI pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery)	1	3	3	**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Blokada portów USB na stacjach roboczych • Dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive
Ataki telefoniczne	• Intruz podający się za „naszego informatyka" prosi o podanie hasła pod pretekstem sprawdzania lub naprawy naszego systemu informatycznego • Intruz przedstawia się jako „serwisant Orange lub Netii" naprawiający usterkę i prosi	1	2	2	**Procedura:** • Szkolenia personelu • Regulamin ODO

	o wejście na określoną stronę internetową w ramach testowania łącza internetowego • Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację" lub prosi o udostępnienie pulpitu • Próba uzyskania informacji o przyznanych świadczeniach/złożonych wnioskach				
Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force): • do systemu WWW (Wordpress) • do poczty elektronicznej • do routerów	2	1	2	**Procedura:** • Metody i środki uwierzytelnienia (polityka haseł) • Szkolenia personelu **Zabezpieczenia:** • Analiza logów systemowych
Łatwo dostępne, łatwe lub standardowe hasła	• Ujawnianie haseł • Nieprawidłowe przechowywanie (karteczki, pliki) • Stosowanie domyślnych haseł producenta • Stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678 • Stosowanie jednego hasła do wielu (często wszystkich) systemów	1	1	1	**Procedura:** • Metody i środki uwierzytelnienia (polityka haseł) • Szkolenia personelu **Zabezpieczenia:** • długość hasła - 8 znaków • hasło zawiera duże, małe litery, cyfry i znaki specjalne • częstotliwość zmiany hasła – 60 dni • mechanizm wymuszenia zmiany hasła • uwierzytelnianie do o aplikacji o stacji roboczych o dysku sieciowego o poczty o blokada ekranu smartfona
Ataki na oprogramowanie - Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu Zagrożenie dla programów • Systemy operacyjne na stacjach roboczych • Systemy serwerowe • Przeglądarki www • Wordpress • Adobe • Flash • Java	1	2	2	**Procedura:** • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • Stosowane jest darmowe/komercyjne oprogramowanie do inwentaryzacji zainstalowanego oprogramowania na stacjach roboczych (serwerach) oraz do kontroli procesu aktualizacji (patche / łatki) • Aktualizacja oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack'i, łatki)
Podsłuch	• podsłuch podczas zdalnego dostępu do sieci wewnętrznej przez Internet	1	1	1	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:**

					• szyfrowanie połączeń internetowych SSL/VPN
Ataki na oprogramowanie - Włamania z wykorzystaniem luk typu zero day	Zero-day to błędy w oprogramowaniu, do których autor nie przygotował jeszcze poprawek / aktualizacji. Informacje o nich są sprzedawane i wykorzystywane przez intruzów	1	1	1	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Oprogramowanie antywirusowe
Włamania z wykorzystaniem API (interfejsów programistycznych)	Niektóre aplikacje pozwalają na zdalne zarządzanie nimi przez specjalnie zaprojektowane funkcje/usługi sieciowe. Np. baza danych może pozwalać na podłączenie się do niej administratorowi w celu wykonania prac naprawczych lub backupu. Dostęp ten odbywa się przy użyciu domyślnych loginów i haseł, co stanowi zagrożenie	1	1	1	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Zmiana domyślnych loginów i haseł • Wyłączenie zdalnego dostępu, gdy nie jest wymagany
Skanowanie sieci i usług	Udostępniane w Internecie serwery, urządzenia sieciowe i aplikacje oraz serwisy www mogą być namierzane przez intruzów poprzez skanowanie adresów IP. Polega to na próbach łączenia się z wszystkimi znanymi usługami w celu sprawdzenia, które z nich są dostępne w naszej sieci i w jakiej wersji. Dzięki temu możliwe jest znalezienie usług nieaktualnych i zawierających błędy	2	2	4	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Firewalle • Wyłączanie niepotrzebnych usług na urządzeniach sieciowych i serwerach
Nieuprawniony dostęp do sieci z użyciem hakerskiego urządzenia	Możliwość wpięcia hakerskiego urządzenia do łatwo dostępnych urządzeń sieciowych wewnątrzorganizacyjnych, celem uzyskania dostępu do sieci przez to urządzenie z zewnątrz. Zagrożenie dla nast. elementów: • gniazdka sieciowe w korytarzach, w sali konferencyjnej	1	2	2	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Okablowanie i elementy sieci są fizycznie zabezpieczone przed ingerencją osób postronnych • Blokada portów USB na stacjach roboczych • Dezaktywacja nieużywanych gniazd sieciowych poprzez wypięcie przewodu lub wyłączenie portu na switchu
Atak ransomeware	Ransomeware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Są też znane przypadki infekcji poprzez sieć lokalną. Odszyfrowanie wymaga zapłaty np. 500 USD. Bardzo groźny	2	2	4	**Procedura:** • Procedura zabezpieczenia systemu informatycznego • Procedura tworzenia kopii zapasowych • **Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenia:** • Systemy antywirusowy i antyspamowy • Kopie bezpieczeństwa kluczowych danych zabezpieczone przed szyfrowaniem przez ransomeware (na nośnikach typu taśmy)

					• blokada dostępu do określonych stron
Atak DOS / DDOS	Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. Atak dotyczy głownie stron i aplikacji www. Np. wypełnienie i wysłanie kilka milionów razy formularza kontaktowego (za pomocą skryptu) i spowodowanie zapełnienia dysku.	1	1	1	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Firewall
Nieuprawniony dostęp lub włamanie do pomieszczeń	Dostęp do: • Budynków • Pomieszczeń biurowych • Archiwów • Serwerowni • Miejsc przechowywania kopii bezpieczeństwa Może skutkować: • dostępem do danych w wersji papierowej • dostępem do plików lub aplikacji lub baz danych • zainstalowaniem nieautoryzowanych urządzeń do dostępu do sieci wewnętrznej • kradzieżą komputerów, nośników	1	2	2	**Procedury:** • Polityka kluczy • Polityka kontroli dostępu **Zabezpieczenia:** • kontrola składowania i wydawania kluczy i kluczy zapasowych • proceduralne ograniczenie dostępu do pomieszczeń osobom nieupoważnionym (zakaz wstępu) • praca personelu sprzątającego w ważnych pomieszczeniach w godzinach pracy i w obecności osób upoważnionych • rozmieszczenie komputerów /drukarek /xero ograniczające dostęp osób nieupoważnionych • dostęp osób nieupoważnionych w obecności osoby upoważnionej • zabezpieczenie dostępu do pomieszczeń (drzwi zamykane na klucz / drzwi ognioodporne / drzwi antywłamaniowe) • zabezpieczenie dostępu do serwerowni (zamek kodowy / drzwi antywłamaniowe/ monitoring) • zabezpieczenie dostępu do archiwum (drzwi zamykane na klucz / pieczęć lakowa) • zabezpieczenie dokumentacji / danych w pomieszczeniach (zamknięte niemetalowe szafy / zamknięte metalowe szafy) • systemy alarmowe / zabezpieczenia antywłamaniowe (system alarmowy / kraty / rolety) • ochrona fizyczna obiektu / pomieszczeń (firma ochroniarska) • monitoring wizyjny w obrębie obiektu i otoczeniu
Kradzież / zagubienie sprzętu i nośników poza organizacją (jeśli dane osobowe występują na tych nośnikach)	Kradzież / zagubienie: • laptopów • smartfonów, • pendrive	1	2	2	**Procedury:** • Regulamin użytkowania komputerów przenośnych • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Szyfrowanie laptopów (bitlocker, Truecrypt, Veracrypt) • Stosowanie szyfrowanych pendrive dla najważniejszych danych • Uwierzytelnianie do urządzeń typu smartfon • Programy do zdalnego blokowania/czyszczenia smartfonów
Nieuprawniony	• brak kontroli nad dostępem do serwera,	1	2	2	**Procedury:**

dostęp do infrastruktury IT oraz do programów	plików, programów, komputerów • nadane zbyt wysokie uprawnienia użytkownikom • dostęp osób nieupoważnionych do kopii bezpieczeństwa • dostęp osób nieupoważnionych do danych prezentowanych na monitorach, drukarkach, kserokopiarkach • niezabezpieczona praca zdalna użytkowników lub serwisu IT				• Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • „obiegówka" jako system zarządzania uprawnieniami • zarządzanie uprawnieniami – profile użytkowników • minimalizacja uprawnień • separacja obowiązków • konta firmowe odseparowane od prywatnych • dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive • praca terminalowa zabezpieczona VPN • blokada logowania się po kilku błędnie podanych hasłach (w systemach udostępniających taką funkcjonalność) **Procedury:** • Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji • Szkolenia personelu • Regulamin ODO **Zabezpieczenia:** • oświadczenia poufności • chronione hasłem wygaszacze ekranu aktywowane po 10 minutach nieaktywności użytkownika • ustawienie monitorów uniemożliwiające wgląd w dane osób postronnych • polityka czystego ekranu
Awarie / uszkodzenia elementów IT	Awarie: • dysków • stacji roboczych • urządzeń sieciowych/routerów • drukarek / skanerów • serwera	1	2	2	**Procedury:** Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** macierze RAID system do inwentaryzacji sprzętu plan ciągłości działania
Błąd / awaria oprogramowania	Awarie: używanych programów komputerowych poczty aplikacji www (Systemu wordpress) bazy danych	1	2	2	**Procedury:** Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** Kopie zapasowe i mechanizm wirtualizacji serwerów

Pożar / eksplozja	Pożar obiektu Pożar serwerowni Pożar serwera	1	2	2	**Procedury:** Zabezpieczenia techniczne **Zabezpieczenia:** gaśnice czujnik dymu w serwerowni
Zalanie	Zalanie archiwum (powódź, zalanie z rur)	1	2	2	**Procedury:** Zabezpieczenia techniczne **Zabezpieczenia:** składowanie dokumentacji papierowej na podwyższeniu
Przegrzanie	wysoka temperatura w serwerowni	1	2	2	**Procedury:** Zabezpieczenia techniczne **Zabezpieczenia:** klimatyzacja w serwerowni
Awaria zasilania	skoki napięcia przerwy w dostawie zasilania	1	2	2	**Procedury:** Zabezpieczenia techniczne **Zabezpieczenia:** UPS podtrzymujący zasilanie serwera UPS na kluczowych elementów systemu IT Agregat prądotwórczy
Nieuprawniona modyfikacja / usunięcie	niezamierzone lub pomyłkowe zmodyfikowanie / usunięcie danych sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji	2	1	2	**Procedury:** Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** Rozliczalność operacji kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych każdy użytkownik programu/systemu posiada swój indywidualny login
Nieuprawnione kopiowanie danych	kopiowanie danych z katalogów, dysków, baz danych, programów kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą	1	1	1	**Procedury:** Procedura zabezpieczenia systemu informatycznego Regulamin ODO **Zabezpieczenia:** Rozliczalność operacji kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych każdy użytkownik programu/systemu posiada swój indywidualny login Blokada portów USB
Nieprzestrzeganie procedur	świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, zapisywanie haseł i umieszczanie ich w widocznym miejscu, naruszenie polityki czystego	1	1	1	**Procedury:** Szkolenia personelu Regulamin ODO

	ekranu lub czystego biurka				
Pomyłki i błędy administratorów, użytkowników	udostępnienia katalogów i dysków z powodu „ułatwienia pracy” administratorów systemów łatwe logowanie się do baz i programów, np. „login admin, hasło admin123” pomyłkowe udostępnienie, wysłanie e-maila do złego odbiorcy, błędne zabezpieczenia	1	1	1	**Procedury:** Procedura zabezpieczenia systemu informatycznego Szkolenia personelu Regulamin ODO
Awaria łączy telekomunikacyjnych	Brak łączności pomiędzy komórkami MOPS oraz dostępu do internetu	1	3	3	Redundancja łączy

DYREKTOR
Miejskiego Ośrodka Pomocy Społecznej
(-) Małgorzata Mruszczyk