Załącznik nr 3 do Polityki Ochrony Danych Osobowych

Arkusz analizy ryzyka RODO

/wzór/

Analiza obejmuje następujące procesy przetwarzania (Zbiory)
1. Kandydaci do pracy, pracownicy
2. Klienci, dostawcy
3. ……

*Legenda: 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** ***UWAGA: Poniższe zagrożenia mają charakter przykładowy. Docelowo należy pozostawić spośród przykładowych zagrożeń te, które faktycznie mogą wystąpić. Przykładowe zagrożenia z poniższej listy, które nie występują należy z tego arkusza usunąć!***	**P**	**S**	**R**	**Zabezpieczenie** ***UWAGA: Poniższe zabezpieczenia mają charakter przykładowy. Docelowo należy pozostawić spośród przykładowych zabezpieczeń te, które są faktycznie stosowane. Przykładowe zabezpieczenia z poniższej listy, które nie są stosowane należy z tego arkusza usunąć!***
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 byłoby w www.rnbank.pl				**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • Sewery proxy i bramki filtrujące o blokada ruchu na podstawie bazy reputacji o blokada dostępu do określonych stron
Nakłanianie do wykonania czynności	• Mail z dyspozycją przelewu wysłany do księgowej z rzekomego konta „Prezesa" • Fax/mail z fakturą od rzekomego „dostawcy" z informacją o zmianie numeru konta bankowego do opłacenia faktur				**Procedura:** • Szkolenia personelu • Regulamin ODO • Wewnętrzny regulamin działu księgowego dotyczący zasad akceptacji i modyfikacji przelewów
Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery). *Najczęściej instalowane są poprzez otwarcie „zainfekowanego" załącznika z maila lub poprzez kliknięcie na zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink (mail z fakturą do opłacenia, mail z DHL o przesyłce, mail z rzekomym pismem urzędowym). W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci* *Działające szkodliwe oprogramowanie może wywołać różnorodne skutki:*				**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • Sewery proxy i bramki filtrujące o skan niebezpiecznej zawartości o blokada ruchu na podstawie bazy reputacji o blokada dostępu do określonych stron

	• *Przejęcie konta pocztowego do wysyłki spamu* • *Użycie przejętych komputerów do kopania kryptowalut* • *Użycie przejętych komputerów do ataków DOS* • *Użycie przejętych komputerów do śledzenia haseł użytkowników celem uzyskania dostępu do systemów i plików* • *Użycie przejętych komputerów do uzyskania pełnego dostępu do wewnętrznej sieci i kopiowania danych i baz danych (kradzież)* *Szkodliwe oprogramowanie:* *Wirusy i trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.* *Backdoory - Instalują się z maili lub z hiperlinków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza.* *Keyloggery - Programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.* *Exploity / exploitpaki - Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.*				
Podrzucone nośniki danych	Atakujący pozostawia w biurze lub w dziale księgowości 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).				**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 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				**Procedura:** • Szkolenia personelu • Regulamin ODO

Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force) : • do baz danych • do serwera • do aplikacji www (np. do wordpressa) • do poczty • do windows na stacjach roboczych • do routera • do firewalla				**Procedura:** • Metody i środki uwierzytelnienia (polityka haseł) • Szkolenia personelu **Zabezpieczenia:** • Testy penetracyjne
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				**Procedura:** • Metody i środki uwierzytelnienia (polityka haseł) • Szkolenia personelu **Zabezpieczenia:** • długość hasła - 12 znaków • hasło zawiera duże, małe litery cyfry lub znaki specjalne • częstotliwość zmiany hasła – 60 dni • mechanizm wymuszenia zmiany hasła • uwierzytelnianie za pomocą kodu PIN / biometryczne • uwierzytelnianie do o aplikacji, o stacji roboczych o dysku sieciowego o sieci o poczty o smartfona • Testy penetracyjne
Ataki na sprzęt - Włamania do urządzeń nieaktualizowanych	Ataki na urządzenia sieciowe oraz inne, które działają dzięki umieszczonemu na nich oprogramowaniu (firmware / sterowniki) Zagrożenie dla nast. elementów: • routery • switche • access pointy • firewall • macierz • dysk NAS • drukarki i skanery *Brak aktualizacji tego oprogramowania (firmware) skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy.*				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Testy penetracyjne • Sondy IPS/IDS
Ataki na sprzęt - Włamania do urządzeń nieodpowiednio skonfigurowanych	Ataki na błędnie skonfigurowany sprzęt lub sprzęt działający z ustawieniami fabrycznymi. Zagrożenie dla nast. elementów: • routery • switche • access pointy • firewall • macierz • dyski NAS				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Zmiana domyślnych haseł na urządzeniach • Zmiana domyślnej nazwy konta administratora w urządzeniu

	• drukarki i skanery *Błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem jest np. pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej routera z poziomu Internetu.*				• Testy penetracyjne
Ataki na sprzęt - Włamania z użyciem niezabezpieczonych interfejsów lokalnych	Atakujący wpina się do urządzeń IT przez ich niezabezpieczone porty konfiguracyjne (USB, Ethernet lub COM - szeregowe) Zagrożenie dla nast. elementów: • routery • switche • firewalle • macierze • serwery • drukarki i skanery *Administratorzy często pozostawiają te porty niezabezpieczone, co powoduje ryzyko wpięcia się do powyższych urządzeń i ich skonfigurowania przez hakera.*				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Dostęp do portów fizycznych (gniazd - np. szeregowy, USB, Ethernet) zabezpieczono hasłem, aby przypadkowa osoba, która podłączy do nich swój komputer nie mogła zmienić konfiguracji. *Zabezpieczenie dostępu do portów fizycznych (np. gniazd szeregowych, USB) za pomocą hasła ma na celu uniemożliwienie dostępu do konfiguracji urządzenia nawet w sytuacji, gdy komuś uda się do niego podłączyć fizyczne. Urządzenie zapyta wówczas o hasło dostępu, podobnie jak w przypadku zdalnej konfiguracji. Domyślnie hasło dostępowe często nie jest wymagane jeżeli mamy bezpośredni dostęp do portów urządzenia, co z punktu widzenia bezpieczeństwa stanowi zagrożenie.* • Umieszczenie krytycznych elementów infrastruktury w zamykanych na klucz szafach serwerowych • Kontrola dostępu do pomieszczeń serwerowni i punktów dystrybucyjnych sieci • Testy penetracyjne
Ataki na sprzęt - Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze)	Atakujący wykorzystuje do włamania usługi sieciowe, których działanie w danym środowisku nie jest wymagane Zagrożenie dla nast. Usług: • DHCP • DNS • SSH • http • telnet • FTP • SMTP • SNMP				**Procedura:** • Procedura wykonywania przeglądów i konserwacji • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Wyłączenie niepotrzebnych serwisów (ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł.)

	Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy.				• Włączone tylko te usługi, które są niezbędne do działania danego środowiska • Monitorowanie aktywnych usług • Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń) • Security Information and Event Managment (analityczny system do wykrywania zagrożeń • Testy penetracyjne
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, Drupal, <inne silniki webowe>, <sklepy internetowe>, • Dedykowany CMS • Adobe • Flash • Java • (podaj inne aplikacje niewymienione) *Istniejące błędy oprogramowania pozwalające na przełamanie zabezpieczeń są upubliczniane po tym, jak producent oprogramowania przygotuje odpowiednią łatę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na atak, np. zdalny dostęp do systemu lub wykonanie złośliwego kodu (instalacja backdoora, exploita, ransomeware)*				**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) • Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń) • Security Information and Event Managment (analityczny system do wykrywania zagrożeń) • Sondy IPS/IDS • Testy penetracyjne
Podsłuch	• podsłuch danych przesłanych drogą mailową • podsłuch danych podczas korzystania z aplikacji webowych • podsłuch podczas korzystania z formularzy kontaktowych • podsłuch podczas zdalnego dostępu do sieci wewnętrznej przez Internet				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • szyfrowanie poczty wysyłanej (SSL) • szyfrowanie połączeń internetowych SSL/VPN • szyfrowanie plików (7zip) wysyłanych mailowo • Ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane

					gniazdka sieciowe (np. sale konferencyjne, korytarze) • Dezaktywacja nieużywanych gniazd sieciowych przez wypięcie przewodu lub wyłączenie portu na switchu *Dezaktywacja gniazdek sieciowych, które nie są używane w danym pomieszczeniu przez komputery i drukarki ma na celu uniemożliwienie podpięcia się do nich intruza z własnym laptopem lub urządzeniem szpiegującym. Gniazda nieużywane powinny być odłączone fizycznie od switcha w szafie, lub konfiguracyjnie poprzez wyłączenie zbędnych portów na switchu.* • Testy penetracyjne
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.				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Oprogramowanie antywirusowe • Sondy IPS/IDS • Testy penetracyjne
Ataki na oprogramowanie - Włamania z wykorzystaniem najczęstszych błędów programistycznych	*Programiści pisząc programowanie często popełniają te same, znane błędy. Przykładowo: możliwość wpisania ujemnej liczby sztuk w formularzu zamówienia, możliwość odgadnięcia numeru zamówienia innego klienta i wpisanie go w pasku adresu przeglądarki w celu wyświetlenia szczegółów.*				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Sondy IPS/IDS • Testy penetracyjne
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.*				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Zmiana domyślnych loginów i haseł • Wyłączenie zdalnego dostępu, gdy nie jest wymagany • Testy penetracyjne
Ataki na oprogramowanie - Namierzanie wersji testowych (np. strona www)	*Niektóre aplikacje posiadają swoje kopie utrzymywane do celów testowych. Są one często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane ze środowiska produkcyjnego. Przykładem może być kopia serwera wykonana w celu przetestowania nowej wersji aplikacji. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl .*				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Zmiana domyślnych loginów i haseł • Stosowanie tych samych zasad bezpieczeństwa, co do systemów produkcyjnych • Testy penetracyjne
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*				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Firewalle

	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.				• Sondy IPS/IDS • Wyłączanie niepotrzebnych usług na urządzeniach sieciowych i serwerach
Włamanie do sieci poprzez WIFI	Uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do sieci bezprzewodowej				**Z Procedura:** • Procedura zabezpieczenia systemu informatycznego **abezpieczenia:** • Odseparowanie wifi dla gości/klientów od sieci wewnętrznej • Stosowanie odpowiednich standardów szyfrowania • Stosowanie mocnych haseł dostępowych

Włamanie z sieci zewnętrznej do sieci wewnętrznej	Włamania z zewnątrz poprzez nieodpowiednio zabezpieczone i skonfigurowane punkty styku z Internetem oraz udostępnione w Internecie serwery i aplikacje.				**Procedura:**
					• Procedura zabezpieczenia systemu informatycznego
					Zabezpieczenia:
					• Sewery proxy i bramki filtrujące
					  ○ skan niebezpiecznej zawartości
					  ○ blokada ruchu na podstawie bazy reputacji
					  ○ blokada dostępu do określonych stron
					• Firewall / NG Firewall / UTM do ochrony dostępu do sieci komputerowej
					  ○ firewall sprzętowy
					  ○ firewall programowy
					• system IDS/IPS do ochrony dostępu do sieci komputerowej
					• Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń)
					• Security Information and Event Managment (analityczny system do wykrywania zagrożeń
					• Testy penetracyjne

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. Możliwość uruchomienia tzw. wrogiego access pointa w celu przechwycenia klientów sieci bezprzewodowej. Zagrożenie dla nast. elementów: • gniazdka sieciowe w korytarzach, w sali konferencyjnej • skanery, drukarki na korytarzach • switche w miejscach dostępnych				**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

					Dezaktywacja gniazdek sieciowych, które nie są używane w danym pomieszczeniu przez komputery i drukarki ma na celu uniemożliwienie podpięcia się do nich intruza z własnym laptopem lub urządzeniem szpiegującym. Gniazda nieużywane powinny być odłączone fizycznie od switcha w szafie, lub konfiguracyjnie poprzez wyłączenie zbędnych portów 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	3	6	**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 (np. utrzymanie poza siecią, najlepiej na nośnikach typu taśmy lub utrzymywanie obrazów-kopii wirtualnych serwerów) • Sewery proxy i bramki filtrujące o blokada ruchu na podstawie bazy reputacji o blokada dostępu do określonych stron
ATAKI MAN-IN-THE-MIDDLE	Zmuszenie komputerów w sieci lokalnej do komunikowania się za pośrednictwem komputera intruza. Umożliwia przechwytywanie i podsłuchiwanie ruchu w sieci.				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Systemy antywirusowe • Sondy IPS/IDS • Systemy SIEM • Testy penetracyjne
Eskalacja uprawnień	• Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych • Przejęcie uprawnień użytkownika zaawansowanego • Przejęcie uprawnień administratora • Przejęcie uprawnień systemowych • Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji)				**Procedura:** • Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • Systemy SIEM • Regularny przegląd logów i uprawnień • Monitorowanie logowania na konta administracyjne • Testy penetracyjne

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. *Zmasowany atak pojedynczego atakującego (DOS) lub z wielu komputerów jednocześnie (DDOS) na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować"*				**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • WAF (Web application firewall) • Firewall • Mechanizm captcha (kod z obrazka do przepisania w formularzu) • Systemy SIEM • Testy penetracyjne
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				**Procedury:** • Polityka kluczy • Polityka kontroli dostępu **Zabezpieczenia:** • kontrola kluczy zapasowych / kontrola wydawania kluczy / kontrola składowania kluczy • portiernia / system przepustek • proceduralne ograniczenie dostępu do pomieszczeń osobom nieupoważnionym (zakaz wstępu) • praca personelu sprzątającego 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 / drzwi zamykane siłownikami) • zabezpieczenie dostępu do serwerowni (drzwi zamykane na klucz / zamki podklamkowe / zamek kodowy / czytnik biometryczny) • zabezpieczenie dostępu do archiwum (drzwi zamykane na klucz / zamek kodowy) • zabezpieczenie dokumentacji / danych w pomieszczeniach (zamknięte niemetalowe szafy / zamknięte metalowe szafy / sejf / sejf ogniotrwały / skrytki na klucze) • systemy alarmowe / zabezpieczenia antywłamaniowe (system alarmowy / kraty / rolety)

					• ochrona fizyczna obiektu / pomieszczeń (ochrona własna / firma ochroniarska) • system kontroli dostępu (wdrożone strefy ograniczonego dostępu / system kart wejściowych / system biometryczny) • 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 • dysków wymiennych				**Procedury:** • Regulamin użytkowania komputerów przenośnych • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Szyfrowanie laptopów (bitlocker, Veracrypt) • Stosowanie szyfrowanych dysków przenośnych • Stosowanie szyfrowanych pendrive • Uwierzytelnianie do urządzeń typu smartfon • Programy do zdalnego blokowania/czyszczenia smartfonów
Nieuprawniony dostęp do infrastruktury IT oraz do programów	• brak kontroli nad dostępem do serwera, plików, programów, komputerów • nadane zbyt wysokie uprawnienia użytkownikom • dostęp osób nieupoważnionych do kopii bezpieczeństwa • łatwy dostęp osób nieupoważnionych do danych prezentowanych na monitorach, drukarkach, kserokopiarkach • niezabezpieczona praca zdalna użytkowników lub serwisu IT				**Procedury:** • Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • szyfrowanie baz danych, aby hacker lub przypadkowy użytkownik nie „widział" danych w bazie • „obiegówka" jako system zarządzania uprawnieniami • program do zarządzania uprawnieniami (np. help desk ze zleceniami administrowania użytkownikami w organizacji) • zarządzanie uprawnieniami – profile użytkowników • program do monitorowania połączeń i działań administratorów / wsparcia technicznego z zewnątrz • minimalizacja uprawnień • separacja obowiązków • konta firmowe odseparowane od prywatnych • separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla wifi i dla Ethernet) np. w salach konferencyjnych

					• dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive • praca terminalowa zabezpieczona VPN • uwierzytelnianie użytkowników z zewnątrz poprzez akceptację wybranych adresów IP • blokada logowania się po kilku błędnie podanych hasłach • Systemy DLP (data leak/loss prevention/protection) *Data Loss Prevention* *Ochrona przed utratą danych (DLP) jest konieczna dla zapobiegania przypadkowym i złośliwym wyciekom istotnych danych, takich jak informacje o klientach, dane finansowe, własność intelektualna lub tajemnice handlowe. Każdy taki incydent może kosztować miliony, doprowadzając do utraty reputacji i klientów, kar finansowych, a nawet spraw sądowych.* *Identyfikowanie, śledzenie i zabezpieczanie wszystkich poufnych informacji: przechowywanych, używanych, a także przesyłanych to prawdziwe wyzwanie dla każdej organizacji. Jest to zadanie coraz trudniejsze z uwagi na wzrastające czynniki ryzyka, do których można zaliczyć: zestresowanych pracowników obawiających się zwolnień, coraz większą mobilność pracowników oraz rosnącą ilość możliwych* **Procedury:** • Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji • Szkolenia personelu • Regulamin ODO **Zabezpieczenia:** • oświadczenia poufności • zahasłowane wygaszacze ekranu aktywowane po XX minutach nieaktywności użytkownika • ustawienie monitorów uniemożliwiające wgląd w dane osób postronnych

					• polityka czystego ekranu • filtry polaryzacyjne na monitorach • drukarki wyposażone w kontrolę wydruków (PIN)
Udostępnianie danych osobom nieupoważnionym z sieci publicznej (przez internet)	• dostęp do danych osobowych poprzez stronę www bez logowania się • dostęp do danych osobowych poprzez stronę www po zalogowaniu się (użytkownik może przeglądać dane osobowe innych użytkowników) • dostęp do katalogów udostępnionych pod publicznym adresem IP plików z danymi osobowymi lub kopii bezpieczeństwa (bez logowania się) • udostępnianie plików zaindeksowanych przez roboty google na skutek braku komend chroniących katalogi webowe przez taką indeksacją • przesłanie lub wydawanie informacji osobie nieupoważnionej				**Procedura** • Procedura wykonywania przeglądów i konserwacji • Regulamin ODO **Zabezpieczenia** • Uwierzytelnianie dostępu do zasobów • Testy penetracyjne • Blokada robotów • Systemy DLP (data leak/loss prevention/protection)
Awarie / uszkodzenia elementów IT	Awarie: • dysków • stacji roboczych • urządzeń sieciowych/routerów • drukarek / skanerów • serwera				**Procedury:** • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • redundancja serwera • macierz RAID • system do inwentaryzacji sprzętu • system do zarządzania licencjami • plan ciągłości działania
Błąd / awaria oprogramowania	Awarie: • programu kadrowo-płacowego • poczty • aplikacji www (np. wordpressa) • bazy danych				**Procedury:** • Procedura wykonywania przeglądów i konserwacji **Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • Wirtualizacja
Pożar / eksplozja	• Pożar obiektu • Pożar serwerowni • Pożar serwera • Zniszczenie serwerowni (np. wybuch gazów technicznych)				**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • gaśnice • system PPOŻ • serwerownia z materiałów niepalnych • czujnik dymu w serwerowni

					• system gaszenia serwerowni gazami technicznymi
Zalanie	• Zalanie serwerowni • Zalanie archiwum (powódź, zalanie z rur)				**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • podłoga techniczna • składowanie dokumentacji papierowej na podwyższeniu • digitalizacja dokumentów archiwalnych
Przegrzanie / zbyt duża wilgotność	• wysoka temperatura w serwerowni • wysoka wilgotność w archiwum				**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • klimatyzacja w serwerowni • powiadamianie administratora systemu informatycznego o alertach temperatury • monitoring środowiskowy w serwerowni - czujnik temperaturowy • monitoring środowiskowy w archiwum - czujniki wilgotności
Awaria zasilania	• skoki napięcia • przerwy w dostawie zasilania				**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • sieć stabilizowana • UPS podtrzymujący zasilanie serwera • UPS na kluczowych elementów systemu IT • Agregat prądotwórczy • Redundantna linia zasilania
Nieuprawniona modyfikacja / usunięcie	• niezamierzone lub pomyłkowe zmodyfikowanie / usunięcie danych • sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji				**Procedury:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Rozliczalność operacji o kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych o każdy użytkownik programu/systemu posiada swój indywidualny login

Nieuprawnione kopiowanie danych	• kopiowanie danych z katalogów, dysków, baz, programów • kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą				**Procedury:** • Procedura zabezpieczenia systemu informatycznego • Regulamin ODO **Zabezpieczenia:** • Rozliczalność operacji o kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych o każdy użytkownik programu/systemu posiada swój indywidualny login • Blokada portów USB • Blokada funkcji eksportu danych w kluczowych programach / systemach
Brak / błędy w wykonywaniu kopii bezpieczeństwa	• doraźne lub za rzadkie wykonywanie kopii • błędy podczas procesu wykonywania kopi • niemożność odtworzenia kopii ze względu na zmiany w oprogramowaniu				**Procedury:** • Procedura tworzenia kopii zapasowych **Zabezpieczenia:** • Wirtualizacja kopii • wykonywany jest backup serwerów / aplikacji / plików / konfiguracji / licencji /haseł • backup jest zabezpieczony przed ransomeware • kopie zapasowe przechowywane są poza serwerownią • testowanie możliwości odtworzenia kopii • niszczenie/czyszczenie nośników przed utylizacją
Nieprawidłowe / brak procedur niszczenia nośników z danymi –	• wyrzucenie uszkodzonych nośników bez ich zniszczenia • wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym • wyrzucenie niezniszczonych , HD, pendrive, DVD				**Procedury:** • Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych **Zabezpieczenia:** • niszczarki paskowe, niszczarki o podwyższonym standardzie • niszczenie/czyszczenie nośników przed utylizacją • firma niszcząca dokumenty
Nieprawidłowe / brak procedur napraw w serwisach	• naprawa sprzętu z nośnikami bez umowy lub bez standardu bezpiecznej naprawy				**Procedury:** • Procedura wykonywania przeglądów i konserwacji

zewnętrznych					
Nieprzestrzeganie procedur	• świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, naruszenie polityki czystego ekranu lub czystego biurka • naruszenia powyżej wskazane na skutek braków w inteligencji lub z powodów niewiedzy				**Procedury:** • Szkolenia personelu • Regulamin ODO
Pomyłki i błędy administratorów, użytkowników	• udostępnienia katalogów i dysków, serwerów ftp, aplikacji z danymi do powszechnego dostępu przez sieć publiczną –z powodu „ułatwienia pracy" administratorów systemów • łatwe logowanie się do baz i programów „login admin, hasło admin1" • dostęp do programów testowych (z prawdziwymi danymi osobowymi) bez logowania • pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia				**Procedury:** • Procedura zabezpieczenia systemu informatycznego • Szkolenia personelu • Regulamin ODO
Błędy projektowe / konfiguracyjne	• błędy programistów prowadzące do udostępniania danych z tworzonych lub administrowanych programów • niezabezpieczenie danych w katalogach i bazach webowych i przed indeksacją robotów google				**Zabezpieczenie** • Procedura zabezpieczenia systemu informatycznego • Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek
Brak aktualnej dokumentacji (instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania)	• Brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania • Brak instrukcji instalacyjnych i konfiguracyjnych środowiska lub oprogramowania *Zagrożenie związane z możliwymi trudnościami w odtworzeniu środowiska i zarządzania nim, gdy np. odejdzie pracownik IT lub będzie on niedostępny podczas krytycznej awarii*				**Procedury:** • Procedury przywracania
Nieprawidłowe / brak umowy o współpracy	Nieprecyzyjnie określone odpowiedzialności we współpracy, co stwarza ryzyko braku zabezpieczeń				**Zabezpieczenia:** • Umowa powierzenia • Pisemne upoważnienia dla podmiotu współpracującego z jasnymi warunkami bezpiecznej pracy z danymi powierzonymi

Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	*Należy uwzględnić, że umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy*				**Zabezpieczenie** • stosowane są Umowy powierzenia • w umowach stosuje się SLA • w umowach stosuje się kary umowne za niewywiązywanie się z realizacji umów • Stosowana jest "Procedura napraw w serwisach zewnętrznych"
Upadek firmy outsourcingowej lub dostawczej	• brak zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji • Utrata usługi / aplikacji, którą świadczy pomiot przetwarzający				**Zabezpieczenie** • Redundancja firmy / osoby
Awaria łączy telekomunikacyjnych	Krytyczne dla administratora świadczącego usługi wymagające „internetu”, usługi chmurowe, ISP oraz dostawcy platform SaaS				• Redundancja łączy