Załącznik nr 6 do Polityki Ochrony Danych
Wykaz zabezpieczeń *-wzór*

Stan na dzień: DD.MM.RRRR

1. Regulamin ODO dla pracowników i współpracowników
• osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych (z Regulaminem ODO)
• osoby zatrudnione przy przetwarzaniu podpisują stosowne Oświadczenie poufności

2. Szkolenia personelu
• szkolenia wewnętrzne
• szkolenia w formie e-learningu

3. Audyty
• realizowana jest Procedura audytu

4. Testy penetracyjne
• realizowane są testy penetracyjne

5. Procedury przywracania w razie incydentu
• stosowana jest "Procedura Plan ciągłości działania"

6. Polityka kluczy / polityka kontroli dostępu
• stosowana jest procedura "Polityka kluczy"
• stosowana jest procedura "Polityka kontroli dostępu"
• kontrola kluczy zapasowych
• zakaz wstępu osobom nieupoważnionym
• kontrola wydawania kluczy
• kontrola składowania kluczy

7. Dostęp do pomieszczeń i sprzętu
• ograniczenie dostępu do pomieszczeń /komputerów /drukarek /xero
• ograniczenie dostępu do pomieszczeń osobom nieupoważnionym
• dostęp w obecności osoby upoważnionej

8. Zabezpieczenie dostępu do pomieszczeń (w tym biurowych)
• drzwi zamykane na klucz
• drzwi ognioodporne
• drzwi antywłamaniowe
• drzwi zamykane siłownikami

9. Zabezpieczenie dostępu do serwerowni
• drzwi zamykane na klucz

• wejście kodowane
• czytnik biometryczny

10. Zabezpieczenie dostępu do archiwum
• drzwi zamykane na klucz

11. Zabezpieczenie dokumentacji w pomieszczeniach
• zamknięte niemetalowe szafy
• zamknięte metalowe szafy
• sejf
• sejf ogniotrwały
• skrytki na klucze

12. Systemy alarmowe / zabezpieczenia antywłamaniowe
• system alarmowy
• kraty
• rolety

13. Ochrona fizyczna obiektu / pomieszczeń
• ochrona własna
• firma ochroniarska

14. Strefy dostępu
• wdrożone strefy ograniczonego dostępu

15. System kontroli dostępu
• system kart wejściowych
• system biometryczny
• portiernia

16. System ppoż.
• system ppoż. w obiekcie
• system gaszenia serwerowni
• gaśnice

17. Monitoring środowiskowy
• w archiwum - czujniki wilgotności
• w serwerowni - czujnik temperaturowy
• powiadamianie administratora systemu informatycznego o alertach temperatury

18. Klimatyzacja
• klimatyzacja w serwerowni

19. Monitoring wizyjny

• monitoring wizyjny w obrębie obiektu i otoczeniu

20. Systemy UPS / agregaty prądotwórcze
• zastosowano UPS podtrzymujący zasilanie serwera
• zastosowano UPS na kluczowych elementów systemu IT

21. Systemy antywirusowy i antyspamowy
• wersja stanowiskowa
• wersja serwerowa
• system licencjonowany
• system aktualizowany online
• funkcja skanowania poczty
• funkcja skanowania portów USB
• wersja na komputery
• wersja na smartfony
• wersja na tablety
• system antyspamowy

22. Sewery proxy i bramki filtrujące
• skan niebezpiecznej zawartości
• blokada ruchu na podstawie bazy reputacji
• blokada dostępu do określonych stron

23. Systemy firewall, NG firewall, UTM
• Firewall / NG Firewall / UTM do ochrony dostępu do sieci komputerowej
• firewall sprzętowy
• firewall programowy

24. Sondy IDS / IPS
• system IDS/IPS do ochrony dostępu do sieci komputerowej

25. Monitorowanie zużycia
• stosowany jest systemy monitorujący stan usług i zasobów krytycznych (serwerów/ baz danych/ urządzeń sieciowych)

26. SIEM - Security Information and Event Managment
• analityczny system do wykrywania zagrożeń

27. Skanery podatności
• stosowany jest system wykrywania słabości i zagrożeń

28. Systemy do inwentaryzacji
• stosowany jest system do inwentaryzacji sprzętu
• stosowany jest system do zarządzania licencjami

• stosowany jest system do monitoringu użytkowników
• stosowany jest system do kontroli smartfonów

29. Szyfrowanie
• szyfrowanie poczty (SSL)
• szyfrowanie połączeń internetowych SSL/VPN
• szyfrowanie pendrive
• szyfrowanie dysków komputerów przenośnych (bitlocker)
• szyfrowanie plików (7zip)
• szyfrowanie baz danych
• szyfrowanie sieci WIFI

30. Hardening
• włączenie szyfrowania
• zmiana domyślnych haseł
• wyłączenie niepotrzebnych funkcji i usług
• dodatki noscript i adblocker do przeglądarek

31. Redundancja krytycznych zasobów
• macierz dyskowa RAID 3
• redundancja łącz

32. Aktualizacje systemu
• zarządzanie aktualizacjami systemu operacyjnego
• zarządzanie aktualizacjami aplikacji
• zarządzanie aktualizacjami przeglądarek internetowych

33. Backupy i archiwizacja
• stosowana jest "Procedura tworzenia kopii zapasowych"
• wykonywany jest backup serwerów / aplikacji / plików / konfiguracji / licencji /haseł
• backup jest zabezpieczony przed ransomeware
• kopie zapasowe przechowywane są poza serwerownią
• niszczenie/czyszczenie nośników przed utylizacją

34. Rozliczalność operacji
• program / aplikacja posiada mechanizm odnotowywania wykonywania operacji na danych osobowych. Odnotowane i logowane są: tworzenie rekordu /zmiana /usunięcie /wgląd w dane / identyfikator użytkownika dokonującego zmianę
• każdy użytkownik posiada swój indywidualny login

35. Postępowanie z nośnikami
• Stosowana jest "Procedura postępowania z nośnikami i sprzętem poza organizacją"
• stosowany jest "Regulamin korzystania z komputerów przenośnych"

• ograniczono możliwość kopiowania danych na pendrive
• zastosowano blokadę portów USB do korzystania z pendrive
• wymuszono użycie szyfrowanych firmowych pendirve

36. Zabezpieczenie pracy użytkowników
• Stosowana jest "Procedura korzystania z internetu"
• Stosowana jest "Procedura korzystania z poczty elektronicznej"
• zahasłowane wygaszacze ekranu aktywowane w przypadku nieaktywności użytkownika
• poufne ustawienie monitorów
• filtry polaryzacyjne
• terminacja sesji

37. Wirtualizacja
• stosowana jest wirtualizacja serwerów

38. Niszczenie nośników
• stosowana jest "Procedura niszczenia nośników"
• niszczarki paskowe
• niszczarki o podwyższonym standardzie
• niszczenie/czyszczenie nośników przed utylizacją
• firma niszcząca dokumenty

39. Zarządzanie uprawnieniami
• stosowana jest "Procedura zarządzania uprawnieniami"
• minimalizacja uprawnień
• separacja obowiązków
• zarządzanie uprawnieniami
• konta firmowe oddzielone od prywatnych

40. Uwierzytelnianie
• stosowana jest "Polityka haseł"
• długość hasła - 12 znakowe z dużymi i małymi literami i znakami specjalnymi
• częstotliwość zmiany haseł ustalono na 60 dni
• wymuszenie zmiany hasła
• użytkownicy zobowiązani są do samodzielnego zmieniania hasła
• uwierzytelnianie za pomocą kodu PIN
• uwierzytelnianie biometryczne
• hasło na BIOS.
• zapewniono uwierzytelnianie do aplikacji/ stacji roboczych/ smartfonów /dysków sieciowych /sieci /poczty

41. Umowy serwisowe
• stosowane są Umowy powierzenia
• w umowach stosuje się SLA

• w umowach stosuje się kary umowne za niewywiązywanie się z realizacji umów

42. Procedury napraw w serwisach zewnętrznych
• Stosowana jest "Procedura napraw w serwisach zewnętrznych"

43. Outsourcing
• korzystanie z ISP
• korzystanie z hostingu poczty /serwera
• wykup cloud-u