Załącznik nr 9 do Polityki Ochrony Danych

Wykaz zabezpieczeń na dzień: 06.06.2019

1. Regulamin Ochrony Danych Osobowych, Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu dla pracowników i współpracowników

- osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych (z Regulaminem Ochrony Danych Osobowych, Polityką Ochrony Danych Osobowych w PWSTE w Jarosławiu, przepisami RODO)
- osoby zatrudnione przy przetwarzaniu podpisują stosowne Oświadczenie poufności

2. Szkolenia personelu

- szkolenia wewnętrzne

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"
- 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

9. Zabezpieczenie dostępu do serwerowni

- drzwi zamykane na klucz
- ograniczenie dostępu do serwerowni

10. Zabezpieczenie dostępu do archiwum

- drzwi zamykane na klucz

11. Zabezpieczenie dokumentacji w pomieszczeniach

- zamknięte niemetalowe szafy
- zamknięte metalowe szafy

- klucze do szaf zamykane w oddzielnych szafkach

12. Systemy alarmowe / zabezpieczenia antywłamaniowe
- rolety

13. Ochrona fizyczna obiektu / pomieszczeń
- ochrona własna
- monitoring wizyjny

14. Strefy dostępu
- wdrożone strefy ograniczonego dostępu

15. System kontroli dostępu
- portiernia

16. System ppoż.
- system ppoż. w obiekcie
- gaśnice

17. Monitoring środowiskowy
- w serwerowni - czujnik temperaturowy
- powiadamianie informatyka o alertach temperatury

18. Monitoring wizyjny
- monitoring wizyjny w obrębie obiektu i otoczeniu

19. Systemy UPS / agregaty prądotwórcze
- zastosowano UPS podtrzymujący zasilanie serwerów
- zastosowano UPS na kluczowych elementów systemu IT

20. Systemy antywirusowy i antyspamowy
- wersja stanowiskowa
- wersja serwerowa
- system licencjonowany
- system aktualizowany online
- funkcja skanowania poczty
- funkcja skanowania portów USB
- system antyspamowy

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

22. Systemy firewall, NG firewall, UTM
- Firewall / NG Firewall / UTM do ochrony dostępu do sieci komputerowej
- firewall sprzętowy
- firewall programowy

23. Sondy IDS / IPS

- system IDS/IPS do ochrony dostępu do sieci komputerowej

24. Monitorowanie zużycia

- stosowany jest systemy monitorujący stan usług i zasobów krytycznych (serwerów/ baz danych/ urządzeń sieciowych)

25. SIEM - Security Information and Event Managment

- analityczny system do wykrywania zagrożeń

26. Skanery podatności

- stosowany jest system wykrywania słabości i zagrożeń

27. Systemy do inwentaryzacji

- stosowany jest system do inwentaryzacji sprzętu
- stosowany jest system do zarządzania licencjami
- stosowany jest system do monitoringu użytkowników

28. Szyfrowanie

- szyfrowanie poczty (SSL)
- szyfrowanie połączeń internetowych SSL/VPN
- szyfrowanie pendrive
- szyfrowanie dysków komputerów przenośnych (bitlocker)
- szyfrowanie sieci WIFI

29. Hardening

- włączenie szyfrowania
- zmiana domyślnych haseł
- wyłączenie niepotrzebnych funkcji i usług
- dodatki noscript i adblocker do przeglądarek

30. Redundancja krytycznych zasobów

- redundancja łącz

31. Aktualizacje systemu

- zarządzanie aktualizacjami systemu operacyjnego
- zarządzanie aktualizacjami aplikacji
- zarządzanie aktualizacjami przeglądarek internetowych

32. 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

33. Rozliczalność operacji

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

34. Postępowanie z nośnikami

• Stosowana jest Procedura postępowania z nośnikami i sprzętem poza uczelnią
• stosowany jest procedura korzystania z komputerów przenośnych"
• ograniczono możliwość kopiowania danych na pendrive

35. 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

36. Wirtualizacja

• stosowana jest wirtualizacja serwerów

37. Niszczenie nośników

• określone zostały procedury niszczenia nośników
• niszczenie/czyszczenie nośników przed utylizacją

38. Zarządzanie uprawnieniami

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

39. Uwierzytelnianie

• stosowana jest "Polityka haseł"
• długość hasła - 8 znakowe z dużymi i małymi literami i znakami specjalnymi
• częstotliwość zmiany haseł ustalono na 32 dni
• wymuszenie zmiany hasła
• użytkownicy zobowiązani są do samodzielnego zmieniania hasła
• zapewniono uwierzytelnianie do aplikacji/ stacji roboczych/ smartfonów /sieci /poczty

40. Umowy serwisowe

• w umowach stosuje się SLA
• w umowach stosuje się kary umowne za niewywiązywanie się z realizacji umów
• Stosowana jest "Procedura napraw w serwisach zewnętrznych"