## Ogólny opis technicznych środków bezpieczeństwa

Aby zapewnić prawidłowość przetwarzania danych osobowych administrator danych osobowych wdraża następujące środki techniczne (stosowanie nw. w jednostkach organizacyjnych Uczelni w zależności od wyników szacowania ryzyka):

1. Fizyczna ochrona pomieszczeń;
	1. bariery fizyczne w dostępie do pomieszczeń, w których przechowywane są zbiory danych osobowych:
		1. pomieszczenie zabezpieczone drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),
		2. pomieszczenie zabezpieczone drzwiami o podwyższonej odporności ogniowej >= 30 min,
		3. pomieszczenie zabezpieczone drzwiami  o podwyższonej odporności na włamanie – drzwi klasy C,
		4. pomieszczenie, w którym okna  zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej,
		5. pomieszczenie, w których przetwarzane są dane, wyposażone są w system alarmowy przeciwwłamaniowy,
		6. pomieszczenie objęte jest systemem kontroli dostępu,
		7. dostęp do pomieszczeń (kluczy do pomieszczeń) objęty jest systemem kontroli dostępu,
		8. dostęp do pomieszczeń kontrolowany jest przez system monitoringu
		z zastosowaniem kamer przemysłowych,
		9. pomieszczenie zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy,
	2. W pomieszczeniu, w którym przetwarzane są dane osobowe, mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika upoważnionego do przetwarzania danych osobowych albo IOD;
	3. fizyczna ochrona serwerowni – klimatyzacja, system przeciwpożarowy, awaryjne zasilanie, zapasowe łącze internetowe;
	4. monitoring wizyjny na terenie Uczelni;
	5. fizyczna ochrona serwerowni – klimatyzacja, system przeciwpożarowy, awaryjne zasilanie, zapasowe łącze internetowe;
	6. monitoring wizyjny na terenie Uczelni.
2. Bariery fizyczne w dostępie do danych osobowych:
	1. zamykanie drzwi pomieszczeń na czas nieobecności pracowników;
	2. przechowywanie dokumentów zawierających dane osobowe w formie papierowej w zamkniętym meblu biurowym, niemetalowej/metalowej szafie lub sejfie;
	3. kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej/metalowej szafie lub sejfie;
	4. dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
	5. dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena;
	6. wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych w systemie informatycznym;
	7. zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w systemie informatycznym zbioru danych osobowych;
	8. dostęp do danych osobowych w systemie informatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
	9. zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu służącego do przetwarzania danych;
	10. zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika;
	11. ochrona danych osobowych na urządzeniach przenośnych (laptopy, smartfony, przenośnych HDD) oraz nośnikach magnetyczne, optyczne i inne poprzez ich zaszyfrowanie;
	12. przechowywane urządzeń przenośnych i nośników danych w zamkniętych na klucz pomieszczeniach i szafach;
	13. kasowanie (trwałe) dane na urządzeniach przenośnych i ww. nośnikach po ustaniu przydatności kopii danych, lub fizyczne zniszczyć nośniki, na których są przechowywane dane osobowe;
	14. przesyłanie danych osobowych drogą elektroniczną tylko w postaci zaszyfrowanej.
3. Ochrona systemów informatycznych, w których przetwarzane są dane osobowe poprzez:
	1. zabezpieczenie przed awariami sieci energetycznych stosowanie:
		1. zasilania sprzętu z dedykowanych linii zasilających,
		2. listwy zasilającej z filtrem przeciwprzepięciowym,
		3. zasilaczy awaryjnych,
		4. wyłączanie napięcia po zakończeniu pracy na stanowisku;
	2. zastosowanie środków ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity;
	3. stosowanie systemu Firewall do ochrony dostępu do sieci komputerowej;
	4. dostęp do Internetu w sieci Intranet możliwy jest na stacjach roboczych, specjalnie chronionych urządzeniem sprzętowym z wbudowanym programem Firewall i translacją adresów NAT;
	5. blokowanie dostępu do systemu w przypadku opuszczenia stanowiska pracy poprzez:
		1. zablokowanie stację roboczej - wylogowanie się z systemu;
		2. aktywację wygaszacza ekranu;
	6. sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez Administratora Systemu Informatycznego/Lokalnego Administratora systemu Informatycznego;
	7. Cyklicznie sporządzane kopie zapasowe kluczowych systemów IT;

Kopie zapasowe tworzy się:

* + 1. codziennie – na koniec dnia kopię wszystkich danych, które uległy zmianie tego dnia,
		2. raz w tygodniu – na koniec tygodnia kopię wszystkich aplikacji,
		3. raz w miesiącu – na koniec miesiąca kopię zarówno danych, jak i aplikacji, w tym także systemu operacyjnego;

Szczegółowe postanowienia dotyczące stosowania technicznych środków bezpieczeństwa w systemie informatycznym zawiera Instrukcja Zarządzania Systemem Informatycznym.