Instrukcja
zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Karkonoskiej Państwowej Szkole Wyższej w Jeleniej Górze

§ 1
Postanowienia ogólne

Celem wprowadzenia instrukcji jest ustalenie ramowych zasad właściwego zarządzania zabezpieczeniami systemu informatycznego oraz ochrony danych osobowych zwanych dalej „danymi" przetwarzanych w tym systemie.

§ 2
Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

1. Dane osobowe przetwarzane są w KPSW z użyciem serwerów, komputerów stacjonarnych i przenośnych.
2. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, ASI (Administrator Systemów Informatycznych) ustala niepowtarzalny login.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym możliwy jest wyłącznie po podaniu przez użytkownika loginu i właściwego hasła dostępu.
4. ASI lub osoba przez niego upoważniona przekazując użytkownikowi login i hasło przeprowadza szkolenie z zakresu pracy w systemie informatycznym oraz bezpieczeństwa danych w systemie informatycznym.
5. Za realizację procedury rejestrowania, aktualizacji oraz wyrejestrowywania użytkowników w systemie informatycznym odpowiedzialny jest ASI.
6. Login wraz z danymi użytkownika podlega wpisowi do rejestru zezwoleń/uprawnień do przetwarzania danych osobowych oraz rejestracji w systemie informatycznym.
7. Użytkownicy nie mogą korzystać z innych loginów niż te, do których są upoważnieni.
8. Login użytkownika nie podlega zmianie, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie jest przydzielany innej osobie.
9. ABI wyznacza dla każdego systemu informatycznego osobę zastępującą ASI, w przypadku jego nieobecności.
10. LADO (Lokalny Administrator Danych Osobowych), informuje ABI o fakcie utraty przez podległą mu osobę uprawnień dostępu do danych osobowych w systemie informatycznym.
11. Login osoby, która utraciła uprawnienia dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

§ 3
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Hasło ustanowione podczas przyznawania uprawnień przez ASI należy zmienić na indywidualne podczas pierwszego logowania się w systemie.
2. Hasło dostępu użytkownika ulega automatycznej zmianie raz na miesiąc. Za jego

zmianę odpowiedzialny jest użytkownik.
3. Hasło składa się z co najmniej ośmiu znaków, zawiera małe i duże litery oraz cyfry lub znaki specjalne.
4. Hasło nie może być udostępniane innym użytkownikom ani przechowywane w miejscach umożliwiających dostęp do niego osobom trzecim.
5. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie ASI.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego logina i hasła dostępu.
8. W przypadku przetwarzania danych osobowych w komputerach przenośnych za bezpieczeństwo danych osobowych w całości odpowiada użytkownik urządzenia.
9. Komputery przenośne, dyski twarde oraz inne wykorzystywane nośniki informacji powinny być zabezpieczone w sposób uniemożliwiający dostęp do danych osobowych osobom postronnym (np. nieuprawniony dostęp, kradzież komputera, szpiegostwo przemysłowe), poprzez wykorzystanie metod i środków kryptograficznych (szyfrowane partycje dysków twardych, szyfrowanie plików, ochrona fizyczna nośników).
10. Stanowiska komputerowe, na których login i hasło nie zapewniają dostatecznej ochrony, zabezpiecza się dodatkowym hasłem (hasło wygaszacza ekranu, hasło BIOSu)
11. Hasła ASI są zdeponowane w sekretariacie rektora w zamkniętej kopercie i podlegają zmianie raz w roku.

§ 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Dane osobowe, których administratorem jest KPSW mogą być przetwarzane z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych Uczelni.
2. Użytkownik przystępujący do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe wpisuje login oraz hasło dostępu, a po uzyskaniu akceptacji uruchamia właściwy program.
3. Użytkownik ma obowiązek wylogowania się lub zablokowania systemu w przypadku nieobecności na stanowisku pracy lub w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim użytkownika.
4. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają zezwolenia do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane.
5. Po zakończeniu pracy należy zamknąć programy i po zastosowaniu odpowiedniej procedury wyłączyć komputer.
6. Wychodząc z pomieszczenia, w którym przetwarzane są dane z systemu informatycznego należy sprawdzić czy zamknięte są okna i wejście do pomieszczenia.
7. Użytkownik niezwłocznie powiadamia ASI o przypadku braku możliwości

zalogowania się na swoje konto oraz LADO w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu, zgodnie z przyjętą procedurą.

8. Osoby użytkujące przenośny komputer, służący do przetwarzania danych osobowych, obowiązane są zabezpieczyć dostęp do komputera hasłem, zachować szczególną ostrożność podczas transportu i przechowywania komputera, nie zezwalając na używanie komputera przez osoby nieupoważnione.
9. Drukarki nie mogą być pozostawione bez kontroli jeśli są lub wkrótce będą drukowane na nich dane osobowe z systemu informatycznego, o ile dostęp osób trzecich do pomieszczeń drukarek nie jest odpowiednio ograniczony.
10. Drukowanie na takich drukarkach jest dopuszczalne o ile otoczenie drukarki jest chronione przed fizycznym dostępem osób nieuprawnionych.
11. Za przechowywanie wydruku zawierającego dane z systemu informatycznego w KPSW odpowiada użytkownik tj. wykonawca wydruku.
12. Wykonawca, który odpowiada za przechowywanie wydruku zawierającego dane z systemu informatycznego, może przekazać wydruk oraz odpowiedzialność za jego przechowanie innej osobie tylko wtedy, gdy jest ona upoważniona do dostępu informacji zawartych na wydruku.
13. Wydruki zawierające dane z systemu informatycznego po zakończeniu pracy powinny być przechowywane w zamkniętych szafach.
14. Wydruki, notatki, kserokopie dokumentów itp. nie wykorzystane a zawierające dane osobowe z systemu informatycznego muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.

§ 5
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Zbiory danych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   2) sporządzania kopii zapasowych zbiorów danych (kopie pełne).
2. ASI odpowiedzialny jest za tworzenie kopii bezpieczeństwa systemu informatycznego, przy czym może on zlecić wykonanie tej kopii wyznaczonej osobie zastępującej np. użytkownikowi komputera.
3. Pełne kopie zapasowe zbiorów danych tworzone są codziennie po zakończonym dniu pracy.
4. W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu.
5. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia gdyby doszło do awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest właściwy ASI.
6. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.
7. W przypadku komputerów stacjonarnych i przenośnych nie będących własnością KPSW, użytkownik systemu ma obowiązek sporządzania kopii zapasowych jak również ochrony nośników informacji. Wymaga się od użytkownika stosowania zasad

dotyczących ochrony danych osobowych przed dostępem osób nieuprawnionych.

§ 6
Sposób, miejsce i okres przechowywania nośników informacji zawierających dane osobowe, w tym kopii zapasowych

1. Okresowe kopie zapasowe wykonywane są na dyskietkach, płytach CD, DVD, kasetach do streamerów lub innych elektronicznych nośnikach informacji. Kopie powinny być przechowywane w innych pomieszczeniach niż te, w których przechowywane są zbiory danych osobowych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Rektor, Kanclerz, Administrator Bezpieczeństwa Informacji, Administratorzy Systemu Informatycznego (ASI) oraz osoba zastępująca ASI.
3. Kopie miesięczne przechowuje się przez okres 12 miesięcy. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
5. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika, za ich zniszczenie odpowiada użytkownik.
6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
7. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.
8. W przypadku braku możliwości zrealizowania procedury zniszczenia nośników informacji, należy fakt ten zgłosić ASI. Po przekazaniu nośników zostaną one zniszczone w ramach środków technicznych Sekcji Obsługi Technicznej, bądź poddane procedurze utylizacji nośników informacji realizowanej przez firmę zewnętrzną.
9. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy należy pozbawić przed naprawą zapisu danych albo naprawiać pod nadzorem ASI.

§ 7
Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania

1. Ruch w sieci komputerowej KPSW jest zabezpieczony przed dostępem z zewnętrznej publicznej sieci przez zastosowanie rozbudowanej ściany ogniowej (firewall). Ruch jest monitorowany przez ASI w celu kontroli przepływu danych między siecią publiczną, a siecią KPSW oraz kontroli działań w sieciach.
2. Na wszystkich stacjach roboczych zainstalowane jest oprogramowanie antywirusowe NOD32.
3. Aktualizacje baz danych pobierane są codziennie do lokalnego repozytorium, z którego aktualizacje pobierane są przez pozostałe komputery.

4. Funkcjonowanie oprogramowania antywirusowego nadzorowane jest centralnie przez oprogramowanie konsoli zarządzającej.
5. Użytkownicy powinni być przeszkoleni w ramach wewnętrznych szkoleń adaptacyjnych, w szczególności z zasad bezpiecznej pracy pozwalających unikać szkodliwego oprogramowania oraz zasad postępowania w przypadku wykrycia, lub podejrzenia działania złośliwego oprogramowania.
6. Oprogramowanie używane w systemie informatycznym w KPSW musi być chronione przed jakąkolwiek niekontrolowaną modyfikacją, nieautoryzowanym usunięciem oraz kopiowaniem.
7. Przed jakimkolwiek zainstalowaniem nowego oprogramowania należy sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
8. W systemie informatycznym w KPSW może być używane wyłącznie oprogramowanie licencjonowane przez posiadacza praw autorskich.
9. Oprogramowanie może być używane tylko zgodnie z prawami licencji.
10. Narzędzia związane z bezpieczeństwem systemów mogą być wykorzystane w systemie informatycznym w KPSW tylko jeśli pochodzą od zaufanego dostawcy.
11. Użytkownik przeprowadza cykliczne kontrole antywirusowe w przydzielonym mu komputerze – minimum raz w miesiącu. W przypadku wykrycia wirusów komputerowych, sprawdzane jest stanowisko komputerowe na którym wykryto wirusa oraz wszystkie posiadane przez użytkownika nośniki
12. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze, w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowaniu.
13. W przypadku podejrzenia wykrycia wirusa komputerowego użytkownik powinien natychmiast powiadomić o tym ASI.
14. Bez zgody ASI zabronione jest instalowanie jakiegokolwiek oprogramowania komputerowego.
15. Pobieranie w niezbędnym zakresie danych ze źródeł zewnętrznych możliwe jest wyłącznie po uprzednim ich sprawdzeniu na obecność wirusów komputerowych.
16. ASI dokonuje zniszczenia uszkodzonego lub zużytego komputerowego nośnika informacji w sposób uniemożliwiający odtworzenie zapisanych na nim danych.

§ 8
Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Udostępnienie danych osobowych instytucjom, osobom spoza Uczelni może odbywać się wyłącznie na pisemny uzasadniony wniosek, za zgodą Rektora lub Kanclerza.
2. ABI prowadzi ewidencję udostępniania danych osobowych.
3. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.
4. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.

§ 9
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Przeglądy i konserwacje systemu oraz informatycznych zbiorów danych wykonuje na

bieżąco ASI. Sprawdzana jest spójność danych, indeksów oraz stan nośników informacji, np. dysków twardych oraz urządzeń peryferyjnych.
2. ASI okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest ustalana przez ABI.
3. Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa została sprawdzona na rynku – z pełnym zastosowaniem procedur obowiązujących w KPSW.
4. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz wyznaczonego przez ASI pracownika, w miejscu jego użytkowania.
5. W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą ASI.
7. W przypadku komputerów stacjonarnych i przenośnych nie będących własnością KPSW użytkownik systemu jest odpowiedzialny za zabezpieczenie danych osobowych znajdujących się na jego komputerze, przed przekazaniem sprzętu do serwisu.
8. W przypadku problemów z realizacją zabezpieczenia danych osobowych, użytkownik systemu zobowiązany jest zwrócić się o pomoc, w tym zakresie, do pracowników Sekcji Informatyzacyjnej.
9. Niesprawne nośniki danych, na których przechowywano dane osobowe powinny być niszczone trwale, aby nie był możliwy odczyt z nich jakichkolwiek danych.
10. Uszkodzone urządzenia i nośniki, które zawierają dane osobowe, powinny być trwale niszczone fizycznie. W przypadku braku możliwości zakupu nowych urządzeń lub nośników oraz odtworzenia utraconych danych z kopii zapasowych, należy podjąć ich naprawę na miejscu w obecności upoważnionego pracownika.
11. W przypadku zbywania/darowizny komputerów lub nośników wykorzystywanych dotychczas przez KPSW wszystkie dane osobowe w nich zawarte powinny być wykasowane nieodwracalnie.
12. Uszkodzone urządzenie lub nośnik nie będący własnością KPSW, na którym znajdują się dane osobowe powinien być trwale niszczony fizycznie lub naprawiany w obecności użytkownika.
13. Osobą odpowiedzialną za okresową weryfikację uprawnień poszczególnych użytkowników aplikacji jest ASI.
14. Każdy system wielodostępny powinien zawierać odpowiednie, automatyczne narzędzia pozwalające ASI na weryfikację stanu bezpieczeństwa systemu.
15. Poszczególne systemy informatyczne powinny w sposób bezpieczny prowadzić zapis wszystkich znaczących zdarzeń systemowych mających wpływ na bezpieczeństwo przetwarzanych w nich danych osobowych a w szczególności:
    1) zmian logina użytkownika w czasie sesji,
    2) prób odgadywania haseł,
    3) prób wykorzystania uprawnień, do których użytkownik nie uzyskał autoryzacji,
    4) modyfikacji oprogramowania aplikacyjnego,
    5) modyfikacji oprogramowania systemowego,
    6) zmian uprawnień użytkowników,

7) prób ingerencji w systemowe rejestry zdarzeń.

16. Rejestry zdarzeń systemowych związanych z bezpieczeństwem systemów informatycznych powinny być przechowywane przez okres co najmniej 1 roku.
17. Podczas tego okresu muszą być zabezpieczone w taki sposób aby nie była możliwa ich modyfikacja oraz aby były one dostępne jedynie dla autoryzowanych pracowników.
18. Co kwartał należy przeprowadzać weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich komputerach podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa. Czynności te winny być dokumentowane przez ASI.
19. ASI co najmniej raz na kwartał winien przeprowadzić weryfikację usług sieciowych dostępnych w systemach informatycznych oraz blokować usługi niewykorzystywane.
20. ASI jest odpowiedzialny za uaktualnianie systemów operacyjnych i aplikacji.
21. ABI lub osoba wyznaczona wraz z ASI raz na miesiąc, a w przypadku podejrzeń naruszenia zabezpieczeń danych osobowych z uwagi na stan urządzeń lub sposób działania programu, bezzwłocznie:
    1) sprawdzają serwer oraz poszczególne komputery za pomocą istniejących w systemie informatycznym programów monitorujących,
    2) dokonują przeglądu i bieżącej konserwacji sprzętu oraz zbioru danych.