

Siedlce, dnia

.....
(imię i nazwisko)

.....
(stanowisko)

.....
(jednostka organizacyjna)

**Oświadczenie
pracownika o zapoznaniu się z pisemną informacją dotyczącą monitoringu w UWS**

Niniejszym oświadczam, że zostałem zapoznany z pisemną informacją dotyczącą zakresu, celów i sposobów zastosowania monitoringu w Uniwersytecie w Siedlcach, co potwierdzam własnoręcznym podpisem.

Jednocześnie zostałem poinformowany, że tekst informacji dotyczącej monitoringu w UWS jest dostępny w Dziale Spraw Pracowniczych, Dziale Organizacji i Zarządzania oraz na stronie internetowej uczelni (obecnie w zakładce Pracownicy/Druki Działu Spraw Pracowniczych).

.....
(podpis pracownika)

Informacja dotycząca zakresu, celów i sposobów zastosowania monitoringu w UWS

Wyciąg z Regulaminu pracy UWS

Monitoring wizyjny

§ 75

1. W celu zapewnienia bezpieczeństwa pracowników oraz ochrony mienia Uniwersytetu, pracodawca prowadzi nadzór nad terenem zakładu pracy oraz terenem wokół zakładu pracy w postaci środków technicznych, umożliwiających rejestrację obrazu.
2. Monitoring jest prowadzony w:
 - 1) budynkach Uniwersytetu i obejmuje:
 - a) ciągi komunikacyjne,
 - b) hole,
 - c) klatki schodowe,
 - d) miejsca postawienia szaf telekomunikacyjnych,
 - e) serwerownię w budynku przy ul. Żytniej 39,
 - f) pomieszczenia użytkowane przez Ośrodek Zarządzania Siecią Komputerową przy ul. 3 Maja 54;
 - 2) teren wokół budynków Uniwersytetu i obejmuje:
 - a) elewacje budynków,
 - b) wejścia główne do budynków,
 - c) wjazdy/wyjazdy na teren Uniwersytetu,
 - d) parkingi.
3. Monitoring prowadzony w Uniwersytecie nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni i pomieszczeń udostępnianych zakładowej organizacji związkowej.
4. Monitoring jest prowadzony za pomocą:
 - 1) kamer rejestrujących obraz;

- 2) rejestratorów wideo zapisujących materiał na dyskach twardej.
5. Pomieszczenia i teren monitorowany są oznaczone w sposób widoczny i czytelny za pomocą odpowiednich znaków (tablic informacyjnych).
6. Uniwersytet przetwarza materiały pozyskane z monitoringu wyłącznie do celów, dla których zostały zebrane.
7. Administratorem danych osobowych zebranych w wyniku monitoringu jest Uniwersytet w Siedlcach. Pełna treść klauzuli informacyjnej jest dostępna w formie dokumentu, na każdej portierni lub recepcji monitorowanego miejsca.
8. Szczegółowe zasady monitoringu wizyjnego są uregulowane w odpowiednim zarządzeniu Rektora UwS w sprawie funkcjonowania i obsługi monitoringu wizyjnego na terenie UwS.

Monitoring stanowisk komputerowych i komputerów przenośnych

§ 76

1. W celu zapewnienia właściwego użytkowania udostępnionych pracownikom narzędzi pracy pracodawca prowadzi kontrolę stanowisk komputerowych lub komputerów przenośnych.
2. Celem prowadzenia monitoringu, o którym mowa w ust. 1, jest:
 - 1) ochrona komputerów przed zagrożeniami sieciowymi i wirusami z sieci i z przenośnych nośników danych;
 - 2) kontrola legalności oprogramowania zainstalowanego na komputerach użytkowników,
 - 3) zapewnienie bezpiecznego i zgodnego z prawem korzystania z sieci internetowej.
3. Sposób kontroli, o której mowa w ust. 2 pkt 1, polega na zainstalowaniu na komputerach użytkowników oprogramowania, za pomocą którego przekazywane są do serwera informacje o zagrożeniach. Kontrola pozwala zlokalizować zagrożony komputer, na którym wystąpiły zdarzenia ataku sieciowego lub wnikięcie wirusa. W następnej kolejności komputer jest sprawdzany przez właściwego pracownika i ręcznie odwirusowywany lub przeinstalowywany.
4. Sposób kontroli, o której mowa w ust. 2 pkt 2, polega na zainstalowaniu na komputerach użytkowników oprogramowania, za pomocą którego dokonywane są cykliczne audyty w zakresie monitorowania oprogramowania zainstalowanego na każdym komputerze. Informacje zebrane w wyniku audytu są przekazywane do serwera i analizowane automatycznie pod kątem zgodności z kluczami oprogramowania wprowadzonymi do bazy programów zakupionych przez uczelnię. Wykryte niezgodności są analizowane. W przypadku wykrycia oprogramowania bez licencji i uznania go za nielegalne informacja przekazywana jest do administratora komputera z poleceniem jego usunięcia z komputera.
5. Sposób kontroli, o której mowa w ust. 2 pkt 3, polega na rejestrowaniu zdarzeń (logów) dotyczących aktywności internetowej użytkowników w internecie zawierających: datę i czas zdarzenia, identyfikator użytkownika, adres przeglądarkanej strony internetowej, adres ip.
6. Dane rejestrowane w trakcie monitoringu są przechowywane zgodnie z zasadami funkcjonowania systemu zarządzania bezpieczeństwem informacji (SZBI) w Uniwersytecie.