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:
		* + 1. ciągi komunikacyjne,
				2. hole,
				3. klatki schodowe,
				4. miejsca postawienia szaf telekomunikacyjnych,
				5. serwerownię w budynku przy ul. Żytniej 39,
				6. pomieszczenia użytkowane przez Ośrodek Zarządzania Siecią Komputerową przy ul. 3 Maja 54;
	2. teren wokół budynków Uniwersytetu i obejmuje:
		* + 1. elewacje budynków,
				2. wejścia główne do budynków,
				3. wjazdy/wyjazdy na teren Uniwersytetu,
				4. 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 twardych.
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**

W celu zapewnienia właściwego użytkowania udostępnionych pracownikom narzędzi pracy pracodawca prowadzi kontrolę stanowisk komputerowych lub komputerów przenośnych.

Celem prowadzenia monitoringu, o którym mowa w ust. 1, jest:

ochrona komputerów przed zagrożeniami sieciowymi i wirusami z sieci
i z przenośnych nośników danych;

kontrola legalności oprogramowania zainstalowanego na komputerach użytkowników,

zapewnienie bezpiecznego i zgodnego z prawem korzystania z sieci internetowej.

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 wniknięcie wirusa. W następnej kolejności komputer jest sprawdzany przez właściwego pracownika i ręcznie odwirusowywany lub przeinstalowywany.

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.

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 przeglądanej strony internetowej, adres ip.

Dane rejestrowane w trakcie monitoringu są przechowywane zgodnie z zasadami funkcjonowania systemu zarządzania bezpieczeństwem informacji (SZBI)
w Uniwersytecie.