

Procedura

**„Postępowanie w przypadku wystąpienia awarii
systemu informatycznego
oraz zasady zgłaszania zdarzeń, incydentów i nieprawidłowej pracy sprzętu”**

1. Cel

Procedura postępowania w przypadku wystąpienia awarii systemu informatycznego ma na celu zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych oraz ochroną krytycznych procesów przed rozległymi awariami lub katastrofami.

2. Awarie systemu informatycznego

Awaria systemu informatycznego - nieprawidłowe działanie systemu informatycznego dotyczące wystąpienia zagrożenia:

1. dostępności danych – brak dostępu do danych dla wszystkich/grupy osób uprawnionych,
2. integralności danych – nieprawidłowe działanie systemu informatycznego skutkujące niezamierzoną utratą lub modyfikacją zgromadzonych danych,
3. poufności danych – nieprawidłowe działanie systemu informatycznego skutkujące ujawnieniem zgromadzonych danych osobom nieuprawnionym.

3. Reagowanie na awarie

3.1. Warunki ogólne

1. Reakcja na awarie musi minimalizować straty, na jakie narażona jest Uczelnia w wyniku danego zdarzenia.
2. Jeżeli charakter awarii pozwala podejrzewać, że może być naruszona poufność danych, należy podjąć działania mające na celu odcięcie źródła danych od drogi komunikacji, przez którą poufność może być naruszona.
3. Informowanie o awariach osób nie będących pracownikami Uczelni wskazane jest jedynie w sytuacji, gdy:
 - a. wymaga tego polskie prawo
 - b. wymaga tego uzyskanie wsparcia spoza Uczelni.
 - c. uzyskano akceptację przekazania informacji o awarii od Administratora Danych.

3.2. Czynności do wykonania

1. Użytkownicy systemu informatycznego zobowiązani są do zgłaszania nietypowych zdarzeń, incydentów oraz nieprawidłowej pracy sprzętu za pomocą systemu Helpdesk dostępnego pod adresem <http://helpdesk.ajd.czyst.pl/> lub w razie braku możliwości skorzystania z ww. systemu telefonicznie/osobiście pracownikom Działu Infrastruktury Informatycznej. Zgłoszenie telefoniczne/osobiste nie zwalnia użytkownika z obowiązku wypełnienia zgłoszenia elektronicznie po uzyskaniu dostępu do systemu Helpdesk.
2. Użytkownicy systemu informatycznego w przypadku powzięcia podejrzenia, że nastąpiło naruszenie ochrony danych osobowych zobowiązani są przekazać Administratorowi danych pisemną informację o wystąpieniu incydentu niezwłocznie, najpóźniej w przeciągu 24 godzin od zaistnienia zdarzenia, wzór zgłoszenia incydentu stanowi załącznik nr 8 „Zgłoszenie wystąpienia incydentu” do obowiązującej na Uczelni Polityki bezpieczeństwa. Administrator ustala czy nastąpiło naruszenie danych osobowych. Jeśli stwierdzi, że nastąpiło, ocenia ryzyko dla osób fizycznych. Jeśli stwierdzi, że naruszenie może narazić prawa i wolności osób fizycznych na ryzyko, powiadamia organ nadzorczy – Urząd Ochrony Danych Osobowych, a w odpowiednich przypadkach również poszkodowane osoby, i ewentualnie przekazuje im informacje o krokach, które mogą podjąć, by chronić się przed konsekwencjami naruszenia. Administrator dokumentuje

naruszenie w rejestrze, wzór rejestru stanowi załącznik nr 9 „Rejestr naruszeń ochrony danych osobowych” do obowiązującej na Uczelni Polityki bezpieczeństwa.

3. Pracownik Działu Infrastruktury Informatycznej otrzymujący zgłoszenie w przypadku, gdy zgłoszenie dotyczy dostępności, integralności, poufności danych informuje o tym zgłoszeniu Administratora Danych, wzór zgłoszenia incydentu stanowi załącznik nr 8 „Zgłoszenie wystąpienia incydentu” do obowiązującej na Uczelni Polityki bezpieczeństwa.
4. Jeżeli podjęta została decyzja o czasowym wyłączeniu części usług systemu informatycznego, należy poinformować o tym fakcie użytkowników tych usług.
5. Jeżeli awaria jest powiązana z celowymi działaniami mającymi na celu zaatakowanie Uczelni, należy rozważyć poinformowanie Policji po konsultacji z Administratorem Danych.
6. Jeżeli system lub dokumentacja (w szczególności Polityka bezpieczeństwa) wymaga wprowadzenia modyfikacji, należy podjąć działania mające na celu ich przeprowadzenie.

4. Rodzaje awarii

4.1. Awarie oprogramowania

1. Jeżeli awaria dotyczy oprogramowania / systemu informatycznego (Egeria, EOD, Płatnik, Arisco, TinLib, Monitoring Wizyjny) należy skontaktować się z Działem Infrastruktury Informatycznej tel. 34 3784251.
2. Jeżeli awaria dotyczy oprogramowania / systemu informatycznego (USOS, CELCAT, SOD, IRK, Platformy E-Learningowej) należy skontaktować się z Zespołem Systemów Informatycznych i Obsługi Dydaktyki tel. 34 3784252.

4.2. Awarie sprzętu

Jeżeli awaria dotyczy sprzętu komputerowego :

1. Jeżeli zgłasza ją pracownik administracji centralnej należy skontaktować się z Działem Infrastruktury informatycznej.
2. Jeżeli zgłasza ją pracownik dydaktyczny lub pracownik administracji wydziałowej należy skontaktować się z informatykiem wydziałowym.