Załącznik nr 1
do Zarządzenia Rektora nr 15/2018
z dnia 25.05.2018 r.

PLAN CIĄGŁOŚCI DZIAŁANIA NA WYPADEK AWARII SYSTEMU INFORMATYCZNEGO W AKADEMII SZTUK PIĘKNYCH W WARSZAWIE

(„procedura")

Cel procedury:

Celem procedury opisanej w niniejszym dokumencie jest minimalizacja zakłóceń w realizacji działalności statusowej Akademii Sztuk Pięknych w Warszawie („jednostka") w związku z wystąpieniem zdarzeń mających wpływ na działanie systemu informatycznego w jednostce.

Procedura opisana w niniejszym dokumencie jest powiązana z procedurami dotyczącymi bezpieczeństwa przetwarzania danych osobowych w ten sposób, iż jej uruchomienie oznacza konieczność przeprowadzenia analizy zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych.

Przedmiot procedury:

Przedmiotem procedury jest określenie sposobu działania w razie zaistnienia zdarzeń mających wpływ na działanie systemu informatycznego.

Osoby zgłaszające:

Każdy użytkownik systemu (pracownik) w razie zaistnienia awarii jest zobowiązany do jej zgłoszenia osobą wskazanym w niniejszej procedurze w celu minimalizacji wpływu awarii na funkcjonowanie jednostki.

Typowe rodzaje incydentów:

a. Awaria serwera;
b. Awaria komputera;
c. Awaria urządzeń aktywnych sieci;
d. Awaria infrastruktury sieciowej;
e. Awaria oprogramowania;

- przy czym przez awarie rozumie się stan niesprawności w/w elementów systemu informatycznego uniemożliwiający jego funkcjonowanie, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie.

Przyczynami powyżej wymienionych zdarzeń mogą być m.in.:

a. umyślne lub nieumyślne działania osób zatrudnionych w jednostce;
b. ingerencja osób zewnętrznych (m.in. atak hackerski);
c. zdarzenia losowe (zanik zasilania, zalanie)

Osoby odpowiedzialne za realizacje procedury:

O uruchomieniu procedury decyduje
- kierownik jednostki;
- Inspektor Ochrony Danych Osobowych,
- kierownicy poszczególnych Działów (po poinformowaniu kierownika jednostki),
- Administrator Systemu Informatycznego.

Plan działania:
- W razie wystąpienia awarii należy wypełnić wszystkie punkty poniższego planu i sporządzić raport, który stanowi załącznik do niniejszego dokumentu.

LP.	Działanie	Opis działania
1)	Zweryfikować zasadność zgłoszenia od użytkownika	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.
2)	Ustalić źródła awarii	Ustalić, co jest przyczyną awarii: • przerwa w zasilaniu prądem, • brak połączenia z siecią Internet, • wadliwe działanie sprzętu, • wadliwe działanie aplikacji, • wadliwe działanie systemu, na którym uruchomiona jest aplikacja.
3)	Określić skalę awarii	Ustalić, czy awaria powoduje zatrzymanie pracy: • jednego pomieszczenia pracy lub działu • kilku pomieszczeń lub działów • całego budynku • wszystkich budynków
4)	Ustalić, czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji	Działanie ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.

5)	Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikację	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer).
6)	Przygotować serwer zastępczy,	Jako serwer zastępczy można wykorzystać np. Komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.
7)	Podjąć decyzję o terminie odtworzenia maszyny	W razie konieczności należy skontaktować się z właściwymi kierownikami komórek organizacyjnych.
8)	Przywrócić funkcjonowanie aplikacji / systemu	Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych.
9)	Sprawdzenie aplikacji / systemu	Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji / systemów zainstalowanych na serwerze.
10)	Uruchomienie usługi w systemie informatycznym Teatru	Po uruchomieniu usługi należy powiadomić właściwych kierowników o tym fakcie.

11)	Określić czy awaria/incydent miała wpływ na przetwarzanie danych osobowych	Określić czy dane osobowe przetwarzane w systemie zostały utracone, zmodyfikowane lub udostępnione osobom postronnym. - poinformować Inspektora Ochrony Danych Osobowych o awarii/incydencie mającym wpływ na dane osobowe - dostarczyć raport z podjętych działań Inspektorowi Ochrony Danych Osobowych - zastosować się do wytycznych Inspektora Ochrony Danych Osobowych

W przypadku wystąpienia awarii/incydentu jest on odnotowywany w dzienniku ASI, który jest niezwłocznie dostarczany Inspektorowi Ochrony Danych Osobowych (dopuszczalna jest forma elektroniczna). Dziennik ASI prowadzony jest na podstawie odrębnych dokumentów obowiązujących w jednostce.

W celu realizacji niniejszej procedury administrator danych osobowych (kierownik jednostki) zapewnia środki materialne i osobowe w celu doprowadzenia do zgodności z przepisami prawa m.in.:

- kontakt z kluczowymi pracownikami działów, lista z numerami telefonów.

- dostęp do najbardziej aktualnej wersji aplikacji,

- dostęp do aktualnej bazy danych,

- zapewnienie środków, dowolnego typu, które w podstawowym zakresie pozwolą na uruchomienie zrealizowanie niniejszej procedury.

Administrator Danych Osobowych może wykonać powyższe przy użyciu Administratora Systemu Informatycznego.

REKTOR
prof. Adam Myjak

WZÓR

PROTOKÓŁ AWARII/INCYDENTU

Nr protokołu ..... , dn .....

1. Termin realizacji czynności: .....
2. Osoba przeprowadzająca: .....
3. Osoby uczestniczące: .....
4. Opis incydentu: .....
5. Podjęte działania: .....
6. Wnioski i rekomendacje: .....

Uwagi:

Podpis osób uczestniczących

Podpis przeprowadzającego