AKADEMIA
ŁOMŻYŃSKA

Załącznik nr 2 do PBI w AŁ

Procedura szacowania ryzyka zasobów IT w Akademii Łomżyńskiej

1. Cel procedury

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia funkcjonowania kluczowych systemów informatycznych Uczelni adekwatnie do zidentyfikowanych zagrożeń mogących mieć wpływ na każdą z cech bezpieczeństwa (poufność, integralność, dostępność) zasobów IT.

2. Identyfikacja zagrożeń i zabezpieczeń

Administrator odpowiedniego zasobu jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w czasie eksploatacji danego zasobu IT.

Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych zasobów.

Wykaz zagrożeń znajduje się w Załączniku nr 1.

Stosowane w Akademii Łomżyńskiej zabezpieczenia mają na celu obniżenie prawdopodobieństwa wystąpienia zagrożeń.

Wykaz zabezpieczeń znajduje się w Załączniku nr 2, stanowiącym dokument wewnętrzny.

3. Szacownie ryzyka dla zagrożeń

Administrator systemu informatycznego (ASI) określa skutki wystąpienia zagrożeń dla każdej z cech właściwego zasobu IT oraz prawdopodobieństwo ich wystąpienia.

Skutki (S) wystąpienia zagrożenia określane są w postaci następującej skali:

1. Małe – brak znaczenia dla badanej cechy lub dotyczy pojedynczych użytkowników.
2. Średnie – wystąpienie incydentu powoduje zaburzenie pracy pojedynczych systemów lub jednostek administracyjnych.
3. Duże – wystąpienie incydentu powoduje zaburzenie pracy całej Uczelni
4. Bardzo duże – wystąpienie incydentu może mieć wpływ na zewnętrzne podmioty.

Prawdopodobieństwo (P) wystąpienia zagrożenia ASI szacuje w oparciu o stosowane zabezpieczenia, dotychczasowe incydenty, obszary dostępności poszczególnych zasobów, stan techniczny sprzętu, prawa gwarancyjne, aktywne umowy serwisowe itp. Prawdopodobieństwo określane jest w następującej skali:

1. niskie – 0,2
2. średnie – 0,4
3. wysokie – 0,6
4. bardzo wysokie – 0,8

Poziom ryzyka (R) dla każdego zagrożenia i cechy określany jest jako iloczyn skutków incydentu oraz prawdopodobieństwa jego wystąpienia (R=S*P). Obliczone ryzyka określane są wg poniższej skali:

0,2 – 0,8 ryzyko niskie – akceptowalne, nie są wymagane dodatkowe czynności,

0,9 – 1,6 ryzyko średnie – zalecane jest rozważenie podjęcia działań mogących obniżyć poziom ryzyka,

1,7 – 2,4 ryzyko duże – wymagane jest podjęcie działań w celu obniżenia poziomu ryzyka,

2,5 – 3,2 ryzyko bardzo duże – wymagane jest natychmiastowe podjęcie działań obniżających poziom ryzyka.

Dla zasobów określonych jako kluczowe, analizę ryzyka należy przeprowadzać nie rzadziej niż raz w roku lub przy wdrażaniu istotnych zmian w zasobie.

Analizę ryzyka przeprowadza się z wykorzystaniem Arkusza analizy ryzyka, którego wzór znajduje się poniżej:

Zasób: (nazwa zasobu)

Cecha	**Zagrożenie**	**Skutki (S)**	**Prawdopodo-bieństwo (P)**	**Ryzyko (R=S*P)**
Poufność	zagrożenie 1	2	0,2	0,4
	zagrożenie 2	1	0,2	0,2
	zagrożenie 3	1	0,2	0,2
	zagrożenie 4	1	0,4	0,4
Dostępność	zagrożenie 1	3	0,2	0,6
	zagrożenie 2	1	0,4	0,4
	zagrożenie 3	1	0,4	0,4
	zagrożenie 4	3	0,2	0,6
Integralność	zagrożenie 1	3	0,2	0,6
	zagrożenie 2	3	0,4	1,2
	zagrożenie 3	4	0,4	1,6
	zagrożenie 4	4	0,8	3,2

4. Postępowanie z ryzykiem

Wyniki analizy ryzyka przedstawiane są Rektorowi. W zależności od wartości ryzyka ASI może proponować wprowadzenie zmian w danym zasobie mających na celu obniżenie zdiagnozowanego ryzyka.

Zmiany obniżające poziom ryzyka, które nie ponoszą za sobą dodatkowych nakładów finansowych i nie zmieniają funkcjonalności zasobu, mogą być wdrażane bez zgody Rektora po konsultacjach z administratorami zasobów współpracujących z modyfikowanym.

Proponowane zmiany, które związane są z ponoszeniem dodatkowych kosztów lub znacząco wpływają na funkcjonowanie zasobu mogą być wdrażane po uzyskaniu akceptacji Rektora.