Załącznik nr 15.10
do Regulaminu konkursu

WYMAGANIA DLA INSTALACJI ELEKTRONICZNYCH SYSTEMÓW OCHRONY (ESO)

1. System ESO w Data Center jest zespołem reguł, procedur i instalacji technicznych, których zadaniem jest kontrola postępowania pracowników oraz zapewnienie bezpieczeństwa obiektu i mienia.
   Na system ESO składają sie z trzy współpracujące ze sobą podsystemy:
   1. System Sygnalizacji Włamania i Napadu (SSWiN).
   2. System Kontroli Dostępu (SKD).
   3. System telewizji dozorowej (CCTV).

2. Normy i przepisy
   Projekt Techniczny instalacji ESO należy wykonać zgodnie z aktualnymi normami i przepisami:

3. Koncepcja ochrony obiektu
   System ochrony musi zarządzać kontrolą do pomieszczeń obiektu w zależności od praw przyznanych pracownikom oraz gościom oraz zapewnić ochronę przed osobami nieautoryzowanymi.

4. Podział budynku STOS CI TASK na strefy bezpieczeństwa

- „Strefa zewnętrzna" - dookoła obiektu z kontrolą ruchu osobowo-materiałowego przez bramę i sygnalizacją naruszenia ochrony obwodowej wokół budynku.
- „Strefa zewnętrznych urządzeń technicznych" – agregaty chłodnicze wody lodowej, kontenery agregatów prądotwórczych, stacje trafo, dodatkowe zbiorniki paliwa (podziemne lub w kontenerach).
- „Strefa wewnętrzna 1" - przedsionek wejściowy z kontrolą ruchu osobowo-materiałowego przez posterunek ochrony obiektu.
- „Strefy wewnętrzne 2" – wspólne korytarze z pomieszczeniami socjalnymi i sanitarnymi, klatki schodowe.
- „Strefy wewnętrzne 3" - pomieszczenia biurowe obsługi, pomieszczenia gospodarcze i techniczne, pomieszczenie ochrony, garaż.
- „Strefy wewnętrzne 4" – rozdzielnia elektryczna, pomieszczenie UPSów, pomieszczenia techniczne na poziomie serwerowym/podziemnym.
- „Strefy wewnętrzne 5" – korytarz i wyjście awaryjne na poziomie serwerowym/podziemnym
- „Strefy wewnętrzne 6" – serwerownie, „bunkier".

6. Wytyczne dla Systemu Sygnalizacji Włamania i Napadu i Kontroli Dostępu
   6.1. System sygnalizacji włamania i napadu (SSWiN) zintegrowany z systemem kontroli dostępu (SKD).
   6.2. System powinien spełniać wymagania Polskiej Normy PN-93/E-08390-14 dla systemów alarmowych klasy SA 4 i urządzeń klasy S oraz wymagania szczegółowe zawarte w normie PNEN-50131-1:2002 (U) oraz PN-EN 50136:2002 (U).
   6.3. System alarmowy powinien obejmować cała powierzchnie Data Center, jak również zewnętrzne otoczenie obiektu, miejsce instalacji modułów i centrali alarmowej w pomieszczeniu chronionym na poziomie serwerowym/podziemnym. Moduły obsługujące elementy wyniesione poza budynek Data Center powinny być wyposażone w izolatory.
   6.4. System SSWN i SKD powinien być zasilany z wydzielonych, oznaczonych pół w rozdzielni głównej, do tych pól nie wolno przyłączać żadnych innych odbiorników energii. Obwody zasilania powinny być zabezpieczone odpowiednio dobranym i oznaczonym

bezpiecznikiem, liczba zabezpieczeń pomiędzy przyłączem energetycznym, a zasilaczami SSWN, nie powinna przekroczyć dwóch.
6.5. Zasilanie rezerwowe systemu (czas zasilania rezerwowego systemu SSWN i SKD powinien wynosić 48 godzin) należy dobrać zakładając całodobowa obsługę (ochronę) oraz świadczenie usług serwisowych w ciągu 24h, system alarmowy powinien nadzorować zarówno zasilacze jak i akumulatory, zasilanie mechanizmów ryglujących powinno posiadać zabezpieczenia zapobiegające uszkodzeniu zasilaczy lub rozładowaniu akumulatorów w przypadku zwarcia w mechanizmie ryglującym.
6.6. Podłączenie systemu do Centralnej Stacji Monitorowania Alarmów Politechniki Gdańskiej powinno być dwutorowe (analogowy dialer telefoniczny, szyfrowany kanał TCP/I).
6.7. W skład systemu powinny wchodzić: czujniki z antymaskingiem, dualne czujniki ruchu, czujniki magnetyczne (drzwi wewnętrzne i zewnętrzne, otwierane okna), czujniki stłuczenia szyby (okna, szklone drzwi), czujniki sejsmiczne, ręczne i radiowe przyciski napadu, bariery lub czujniki ochrony obwodowej.
6.8. System kontroli dostępu bazujący na kontrolerach drzwi powinien spełniać wymagania Polskiej Normy PN-EN-50133:2002 (U). W systemie należy zastosować podstawowe funkcje kontroli dostępu z rejestracją zdarzeń, wykorzystaniem pasywnych kart zbliżeniowych bliskiego zasięgu czytników zbliżeniowych i klawiatur (PIN), czujników biometrycznych oka oraz zaawansowanych funkcji kontroli dostępu: lokalizacja użytkownika w obiekcie, funkcja DOTL (drzwi zbyt długo otwarte), dwie karty otwierają drzwi (karta gościa + karta obsługi), śluza, anti-passback (wymuszanie kolejności wejścia/wyjścia).
6.9. System musi posiadać zabezpieczenie kodem bezpieczeństwa uniemożliwiającym odczytanie karty przez nieautoryzowany czytnik.
6.10. System musi pozwalać na pełne zarządzanie SSWiN i SKD z dedykowanego komputera poprzez sieć TCP/IP (z możliwością samodzielnego programowania kart zbliżeniowych).
6.11. Ograniczenie dostępu do stref ochrony powinno być realizowane wg poniższych wytycznych:

- „Strefa zewnętrzna” - kontrola ruchu osobowo-materiałowego przez posterunek ochrony Data Center, videodomofon przy drzwiach zewnętrznych oraz bramie ze sterowaniem otwarcia drzwi i bramy, interkom na stanowisku ochrony, kontrola dwustronna drzwi i bramy (karta), funkcja DOTL
- „Strefa zewnętrznych urządzeń technicznych” – drzwi z kontrolą jednostronną.
- „Strefa wewnętrzna 1” - kontrola ruchu osobowo-materiałowego przez posterunek ochrony Data Center, drzwi z kontrolą jednostronną (czujnik biometryczny oka).
- „Strefa wewnętrzna 2”- brak kontroli dostępu.
- „Strefa wewnętrzna 3” - drzwi z kontrolą jednostronną (karta), wyjście klamka, możliwość czasowego wyłączenia kontroli za pomocą przycisku przez dowolną osobę zajmującą pomieszczenie.
- „Strefa wewnętrzna 4” - kontrola jednostronna (karta), wyjście na przycisk.
- „Strefa wewnętrzna 5” - kontrola dwustronna (karta).
- „Strefa wewnętrzna 6” - kontrola dwustronna (wejście czujnik biometryczny oka + karta, dwie karty, wyjście karta), funkcja DOTL, funkcja śluza (drzwi pomieszczenia Data Center), funkcja anti-passback.

6.12. Zazbrojenie i rozbrojenie poszczególnych stref musi odbywać się przez uprawnionych użytkowników z manipulatora lub przez posterunek ochrony Data Center.
6.13. Szczególny nacisk należy położyć na bezpieczeństwo ewakuacji przy stosowaniu kontroli dwustronnej, jak również na niezawodność pracy mechanizmów ryglujących.

7. Wytyczne dla systemu telewizji dozorowej (CCTV)

7.1. Obiekt Data Center powinien zostać wyposażony w system telewizji kolorowej IP z rejestracją obrazu, obejmujący wewnętrzne przejścia pomiędzy strefami bezpieczeństwa: przedsionek wejściowy, korytarze wewnętrzne, wejście do pomieszczenia Data Center,

wejścia do serwerowni i bunkra, wnętrze serwerowni i bunkra (przejścia wzdłużne i poprzeczne), zewnętrzne wejście do obiektu, obszar agregatów chłodniczych, wejście w ogrodzeniu, teren obejmujący kontenery z agregatem prądotwórczym i zbiornikiem paliwa.
7.2. System powinien być wyposażony w serwer monitoringu IP zapewniający ciągły zapis wszystkich zaprojektowanych kamer w pełnej rozdzielczości przez co najmniej 30 dni.
7.3. Serwer monitoringu powinien pozwalać na podgląd wybranych kamer autoryzowanym klientom przy pomocy przeglądarki internetowej.
7.4. Zastosowane kamery powinny być w wersji wandaloodpornej współpracujące z projektowanym serwerem monitoringu
7.5. Wszystkie kamery zewnętrzne powinny być w wersji dzień-noc z mechanicznym filtrem podczerwieni, z oświetlaczem podczerwieni, posiadać przetwornik o rozdzielczości 5MP lub większy oraz pracować w temperaturze -30 do 50 stopni i posiadać zabezpieczenie przeciwprzepięciowe.
7.6. Wszystkie kamery wewnętrzne powinny być w wersji kopułkowej, z oświetlaczem podczerwieni, posiadać przetwornik o rozdzielczości 3MP lub większy.
7.7. Wszystkie kamery powinny być wyposażone w obiektywy z automatyczną przysłoną i ręcznym zoom'em dobrane tak aby była możliwa obserwacja wybranych przestrzeni
7.8. Zasilanie kamer wewnętrznych i zewnętrznych powinno być realizowane z przełącznika PoE wyposażonego w co najmniej dwa zasilacze podłączone do dwóch niezależnych obwodów centralnego UPSa.
7.9. Serwer monitoringu powinien być zainstalowany w szafie Rack w pomieszczeniu chronionym na poziomie serwerowym/podziemnym.
7.10. Do podglądu obrazu system powinien posiadać dwa zestawy składające się ze stacji roboczej wyposażonej w 2 monitory TV 4K o przekątnej co najmniej 55”. Jeden taki zestaw powinien być w pomieszczeniu ochrony, drugi w pomieszczeniu operatorów CITASK (NOC CI TASK).
7.11. Należy zapewnić dostęp do systemu telewizji dozorowej dla innych systemów informatycznych zlokalizowanych wewnątrz budynku oraz dla Centralnej Stacji Monitorowania Alarmów Politechniki Gdańskiej.

8. Integracja systemów ESO oraz innych systemów
W celu zapewnienia wysokiego poziomu bezpieczeństwa należy dokonać pełnej integracji wszystkich systemów pracujących w obiekcie, mających wpływ na stan bezpieczeństwa obiektu. Komunikację TCP/IP pomiędzy poszczególnymi systemami, należy zrealizować jako wydzielony segment okablowania strukturalnego Data Center.
8.1 Integracja z Systemem Sygnalizacji Włamania i Napadu (SSWN)
- Wyświetlanie i pełna obsługa zdarzeń alarmowych na stanowisku ochrony Data Center oraz stanowisku NOC-CI TASK w formie map graficznych w celu dokładnej lokalizacji zdarzenia,
- Monitorowanie aktywnych kart użytkowników z wyświetlaniem zdjęć zapisanych w systemie na stanowisku Ochrony oraz NOC-CI TASK
- Zapisywanie zdarzeń alarmowych w bazie danych gromadzonych na serwerze,
- Programowanie centrali alarmowej.

8.2 Integracja z Telewizyjnym systemem dozorowym (CCTV)
- Powiązanie zdarzeń alarmowych oraz aktywnych kart użytkowników z wyświetlaniem rzeczywistego obrazu z danej kamery,
- Weryfikacja wizyjna rejestru zdarzeń wraz z odtwarzaniem obrazów zapisanych na dysku rejestratora,
- Funkcja przyspieszonego zapisu obrazu w czasie alarmu,

8.3 Integracja z Systemem sygnalizacji pożaru (SAP) oraz systemami gaszenia gazem

- Weryfikacja zdarzeń alarmowych na mapie graficznej wyświetlanej na stanowisku ochrony Data Center oraz stanowisku NOC CI TASK i powiązanie ich z wyświetlaniem obrazu z danej kamery,
- Powiązanie sygnałów pożaru / gaszenia gazem z czujnikami otwarcia drzwi podczas ewakuacji w systemie kontroli dostępu.