Akademia Górniczo-Hutnicza im. Stanisława Staszica
w Krakowie

PLAN OCHRONY INFORMACJI NIE JAWNYCH W AGH-D17

Spis treści

1. Wstęp

1.1. Cel planu

Celem niniejszego planu jest zapewnienie skutecznej ochrony informacji niejawnych poprzez określenie zasad, procedur oraz środków organizacyjnych i technicznych, które minimalizują ryzyko ich utraty, ujawnienia lub nieuprawnionego dostępu. Plan uwzględnia specyfikę wyznaczonego obszaru oraz obowiązujące przepisy prawa, w tym ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz akty wykonawcze, a także wyniki analizy poziomu zagrożeń i oceny ryzyka.

Niniejszy plan ochrony informacji niejawnych określa:

- Zasady wytwarzania i przetwarzania informacji niejawnych
- Analiza zagrożeń
- Procedury działania osób odpowiedzialnych za ochronę informacji niejawnych w sytuacji szczególnych
- Opis stref ochronnych i ich granice
- System kontroli dostępu do stref

- Zarządzanie uprawnieniami dostępu
- Opis zastosowanych środków bezpieczeństwa fizycznego

1.2. Podstawy prawne

Podstawą prawną do opracowania niniejszego planu i nadzorowania jego realizacji jest:

- art. 15 ust. 1. pkt 5 ustawy z dnia 05 sierpnia 2010r. o ochronie Informacji niejawnych (Dz.U. 2019 poz. 742)
- § 9 ust. 1 rozporządzenia Rady Ministrów z dnia 29 maja 2012r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U.2012.poz. 683)

1.3. podstawowe definicje (art. 2 UoOIN – ust. 1-5 oraz 15-17).

- ustawa - ustawa z dnia 05 sierpnia 2010 r. o ochronie informacji

- rozporządzenie - rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.

2. Zasady wytwarzania i przetwarzania informacji niejawnych.

2.1. Ogólne postanowienia

Informacje niejawne oznaczone klauzulą „zastrzeżone” są objęte szczególną ochroną w celu zapobieżenia ich nieuprawnionemu ujawnieniu, co mogłoby zaszkodzić interesom Rzeczypospolitej Polskiej.

Ochrona informacji niejawnych reguluje cały proces przetwarzania, od wytworzenia, przez przechowywanie, aż po archiwizowanie lub niszczenie.

2.2. Proces wytwarzania dokumentów zawierających informacje niejawne

Każdy dokument niejawny powinien być sporządzany w brulionach lub innych nośnikach uprzednio zarejestrowanych w dzienniku ewidencji.

Dokumenty są opatrzone odpowiednimi klauzulami tajności, zgodnie z rozporządzeniem Prezesa Rady Ministrów, oraz oznaczeniami zawierającymi sygnatury literowo-cyfrowe.

Sporządzenie dokumentu wymaga:

- Przyznania klauzuli przez osobę upoważnioną.
- Opisu pierwszej i kolejnych stron zgodnie z zasadami oznaczania dokumentów, w tym liczby załączników i ich klauzul.

2.3. Przetwarzanie dokumentów z wykorzystaniem sprzętu komputerowego

Informacje niejawne mogą być przetwarzane wyłącznie na stanowiskach komputerowych przeznaczonych do tego celu, wyposażonych w odpowiednie zabezpieczenia teleinformatyczne.

Komputer po zakończeniu pracy jest odłączany od sieci elektrycznej i przechowywany w zamkniętym pomieszczeniu.

System teleinformatyczny przeznaczony do przetwarzania informacji niejawnych wymaga akredytacji oraz zgodności z dokumentacją bezpieczeństwa.

2.4. Środki bezpieczeństwa

Informacje niejawne przechowywane są w metalowych szafach lub innych zabezpieczonych meblach, które po zakończeniu pracy muszą być zamykane na klucz.

Dostęp do dokumentów jest ograniczony do osób posiadających odpowiednie upoważnienia oraz poświadczenia bezpieczeństwa.

2.5. Ewidencja i obieg dokumentów niejawnych

Dokumenty wytwarzane i otrzymywane są rejestrowane w dzienniku ewidencji. Każdy dokument posiada unikalny numer ewidencyjny poprzedzony literą „Z” oznaczającą klauzulę „zastrzeżone”.

Obieg korespondencji niejawnej jest ściśle kontrolowany i rejestrowany, a odbiór dokumentów wymaga potwierdzenia.

2.6. Archiwizowanie i niszczenie materiałów niejawnych

Materiały niejawne są klasyfikowane i przechowywane zgodnie z rozporządzeniami dotyczącymi dokumentacji archiwalnej.

Dokumentacja niearchiwalna podlega brakowaniu po zakończeniu okresu przechowywania, przy czym niszczenie odbywa się w sposób uniemożliwiający odtworzenie treści.

3. Opis stref ochronnych, w których przetwarza się informację o klauzuli „Zastrzeżone” i „Poufne”

3.1. Strefy ochronne

W budynku D17 tworzy się strefy ochronne z wyszczególnieniem na pomieszczenia 3.23, 3.24, 3.26 stanowiące również pomieszczenia Planu Ochrony Informacji nie jawnych:

- Strefy ochrony II obejmują pomieszczenia Kancelarii Tajnej (pokój 3.24), Czytelni (pokój 3.23) oraz Pomieszczenie Pełnomocnika Ochrony Informacji Niejawnych.
- Strefy ochrony III obejmują wszystkie pozostałem obiekty znajdujące się na terenie placówki.

3.1.1. Strefa ochronna III

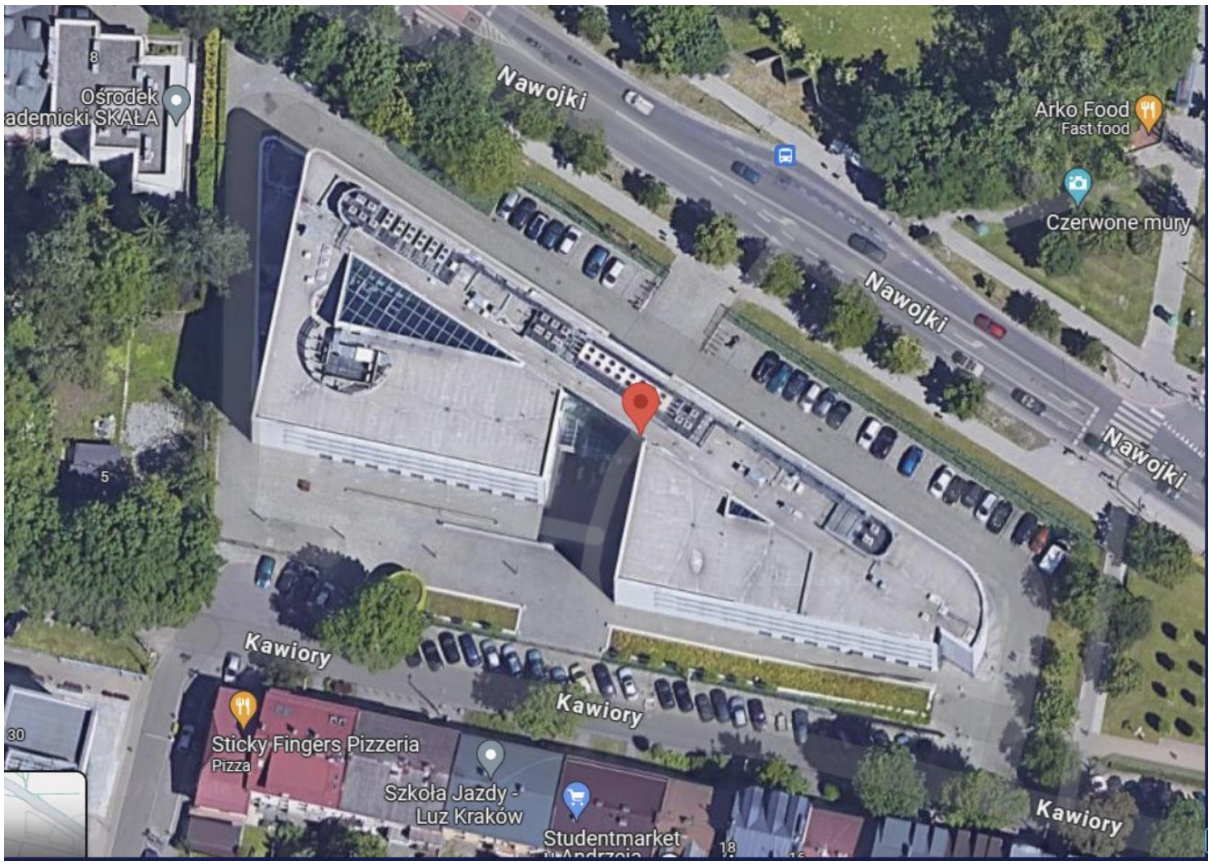
Granice Strefy III

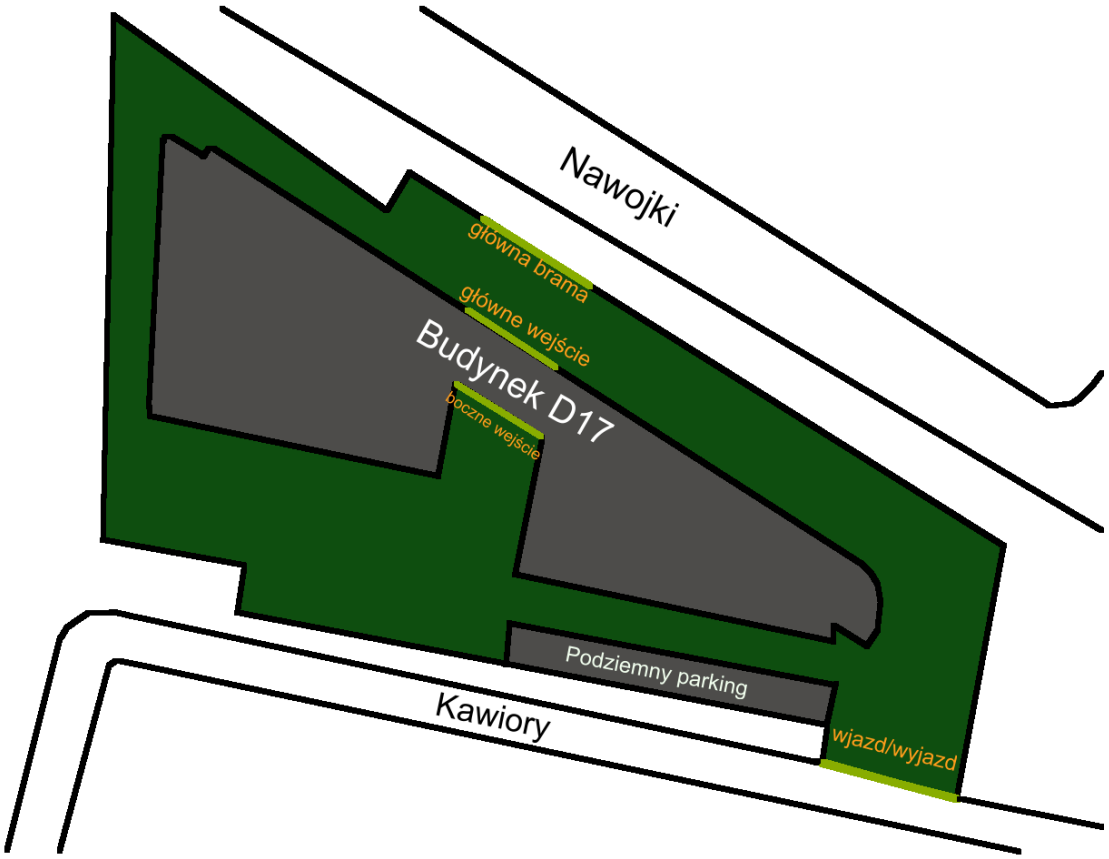
Zewnętrzne granice obszaru:

- Ogrodzenie: Stalowa siatka o wysokości minimum 2,5 metra z dodatkowymi zabezpieczeniami, takimi jak drut kolczasty.
- Wejścia i wjazdy: Bramki wejściowe oraz bramy wjazdowe stanowiące jedyne punkty dostępu do Strefy III, wyposażone w systemy sterowania elektronicznego oraz możliwość blokady.

Granica wewnętrzna z Strefą II:

Przejścia do Strefy II zabezpieczone systemami kontroli dostępu, takimi jak czytniki kart RFID i skanery biometryczne.


Nawojki
Ośrodek
ademicki SKAŁA
Arko Food
Fast food
Czerwone mury
Nawojki
Nawojki
Kawiory
Kawiory
Sticky Fingers Pizzeria
Pizza
Szkoła Jazdy -
Luz Kraków
Studentmarket
Kawiory



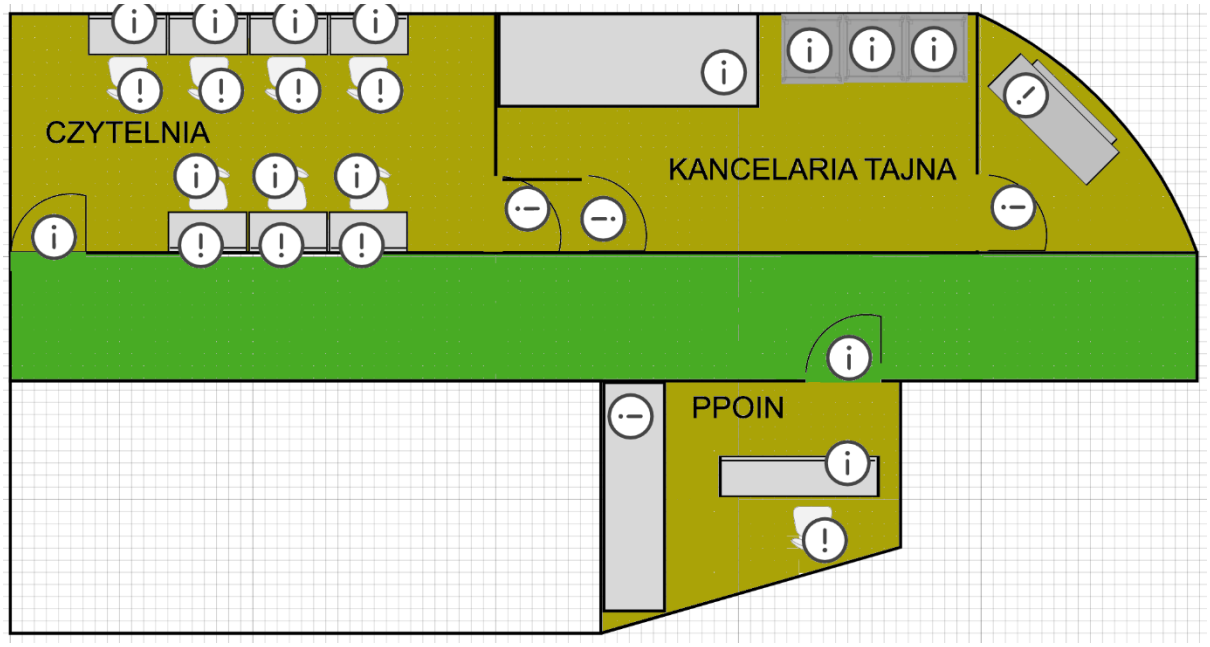
3.1.2. Strefa ochronna II

Przejścia wewnętrzne:

- Wejście do Strefy II: Wyłącznie z terenu Strefy III poprzez drzwi wyposażone w podwójne zamki i śluzy bezpieczeństwa.
- Śluzy bezpieczeństwa: Mechanizm uniemożliwiający jednoczesne otwarcie drzwi prowadzących do i ze strefy.

System kontroli dostępu:

- Granica wyposażona w czytniki kart dostępu, skanery biometryczne oraz rejestratory czasu i danych osób wchodzących i wychodzących.



3.2. System kontroli dostępu do stref

System kontroli dostępu do stref ochronnych opiera się na rygorystycznych zasadach, które mają na celu ograniczenie dostępu wyłącznie do osób posiadających odpowiednie uprawnienia. Wejście do Strefy II i Strefy III jest możliwe jedynie po wcześniejszym potwierdzeniu tożsamości oraz sprawdzeniu uprawnień w rejestrze osób dopuszczonych do przetwarzania informacji niejawnych.

Dla Strefy III zastosowano system identyfikacji osób, który wymaga okazania dokumentów tożsamości i uprawnień przy każdym wejściu. Punkty kontrolne, takie jak stróżówki wyposażone w elektroniczne zamki i systemy komunikacji, stanowią pierwszą linię ochrony.

W przypadku Strefy II obowiązują dodatkowe mechanizmy zabezpieczeń, w tym elektroniczne systemy dostępu, takie jak czytniki kart magnetycznych oraz skanery biometryczne. Wszystkie przejścia do Strefy II

wyposażono w śluzy bezpieczeństwa, które uniemożliwiają jednoczesne otwarcie drzwi, oraz system rejestracji wejść i wyjść, zapisujący czas oraz dane osoby wchodzącej i opuszczającej strefę. Dzięki integracji z monitoringiem CCTV zapewniona jest pełna weryfikacja tożsamości oraz ciągły nadzór nad przestrzenią.

3.3. Zarządzanie uprawnieniami dostępu

3.3.1. Prawo przebywania w strefie III

Prawo przebywania w Strefie III przysługuje wyłącznie osobom, które posiadają odpowiednie uprawnienia wynikające z posiadania certyfikatu bezpieczeństwa osobowego oraz upoważnienia wydanego przez Pełnomocnika ds. Ochrony Informacji Niejawnych. Osoby takie są zobowiązane do przestrzegania zasad bezpieczeństwa obowiązujących na terenie strefy, w tym rejestracji każdorazowego wejścia i wyjścia.

3.3.2. Prawo przebywania w Kancelarii Materiałów Niejawnych

Do kancelarii dostęp mają jedynie osoby upoważnione, które pełnią obowiązki związane z wytwarzaniem, przechowywaniem lub obiegiem dokumentów niejawnych. Wejście do kancelarii wymaga uprzedniego zgłoszenia oraz rejestracji, a obecność osób trzecich jest ściśle zabroniona.

3.3.3. Prawo przebywania w Czytelni Materiałów Niejawnych

Czytelnia Materiałów Niejawnych jest dostępna dla osób, które uzyskały zgodę na zapoznanie się z dokumentami objętymi klauzulą tajności. Przebywanie w czytelni odbywa się wyłącznie pod nadzorem osoby odpowiedzialnej za jej obsługę. Każdorazowe korzystanie z materiałów musi być zarejestrowane w dzienniku użytkowania, a wniesienie urządzeń elektronicznych jest zakazane.

3.3.4. Prawo przebywania w Pomieszczeniu Pełnomocnika Ochrony Informacji Niejawnych

Pomieszczenie Pełnomocnika Ochrony Informacji Niejawnych przeznaczone jest dla osoby pełniącej tę funkcję oraz osób upoważnionych do współpracy w zakresie ochrony informacji niejawnych. Dostęp do tego pomieszczenia wymaga zgody Pełnomocnika i jest rejestrowany w systemie kontroli dostępu.

3.4. Opis zastosowanych środków bezpieczeństwa fizycznego

3.4.1. Strefa III

System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych (§4 ust.3).

Zewnętrzne bariery:

- Ogrodzenia z siatki stalowej o wysokości minimum 2,5 metra z dodatkowym zabezpieczeniem w postaci drut kolczasty.
- Bramy wjazdowe sterowane elektronicznie z możliwością blokady w sytuacjach kryzysowych.

Punkty kontrolne:

- Stróżówki z pancernymi szybami i systemami komunikacji radiowej.
- Fizyczne oddzielenie wjazdu dla pojazdów od wejścia dla pieszych.

Kontrola osób:

- Obowiązek okazywania dokumentów tożsamości oraz uprawnień przy każdym wejściu.
- Stosowanie procedur losowego sprawdzania zawartości bagażu osobistego lub toreb.

Monitoring CCTV:

- Kamery o wysokiej rozdzielczości z funkcją noktowizji.
- Nagrania przechowywane przez minimum 30 dni

Oświetlenie:

- Mocne reflektory LED oświetlające cały obszar strefy przez całą dobę.
- Automatyczne czujniki ruchu aktywujące dodatkowe źródła światła w przypadku wykrycia obecności.

Alarmy:

- System alarmowy reagujący na nieautoryzowane próby wejścia lub ingerencję w infrastrukturę strefy.

3.4.2. Strefa II

Fizyczne bariery:

- Ściany wykonane z materiałów o wysokiej odporności na włamania, beton zbrojony.

- Wewnętrzne przegrody uniemożliwiające dostęp do kluczowych elementów infrastruktury, systemów informatycznych.
- Zabezpieczenia drzwi, okien i innych punktów dostępu
- Meble ochrony sejfy na dokumenty niejawne.

Mechanizmy kontroli dostępu:

- Elektroniczne zamki drzwi z czytnikami kart magnetycznych lub RFID.
- Skanery biometryczne (np. odciski palców, rozpoznawanie twarzy) dla wybranych osób o najwyższych uprawnieniach.

Rejestracja wejść i wyjść:

- Automatyczne zapisywanie w systemie czasu i danych osoby wchodzącej oraz wychodzącej.
- Integracja z monitoringiem CCTV dla potwierdzenia tożsamości.

Śluzy bezpieczeństwa:

- Drzwi prowadzące do Strefy II wyposażone w podwójne zamki, uniemożliwiające jednoczesne otwarcie obu przejść.
- Pomieszczenia przedsionków monitorowane za pomocą systemów CCTV z dostępem tylko dla personelu kontrolującego.

Tabliczki ostrzegawcze:

- Widoczne oznaczenia strefy, np. „STREFA OCHRONNA II – WSTĘP OGRANICZONY” umieszczone przy wejściach.
- Informacje o obowiązujących zasadach, takich jak zakaz wnoszenia urządzeń elektronicznych.

4. Analiza Zagrożeń

Za ochronę informacji niejawnych i funkcjonowanie systemu ochorny w AGH-D17 odpowiada Pełnomocnik ds. Ochorny Informacji Niejawnych. Do personelu bezpieczeństwa w zakresie przetwarzania informacji niej

4.1. Zagrożenia zewnętrzne

Zagrożenia zewnętrzne należy rozpatrywać w trzech aspektach:

- działań sabotażowych;
- działań terrorystycznych;
- działań kryminalnych.

Działalność ta może być prowadzona poprzez:

- pozyskiwanie informatorów spośród zatrudnionych pracowników;
- umieszczenie informatora wśród nowo zatrudnionych;
- instytucję przykrycia np. firmę wykonującą jakiekolwiek prace w obiekcie;
- penetrację obiektu z prowadzeniem obserwacji bezpośredniej, inwigilacji
- zatrudnionych w obiekcie oraz wykorzystanie środków technicznych;
- próby zdobycia dokumentów niejawnych przez sforsowanie zabezpieczeń technicznych oraz ominięcie (unieszkodliwienie) systemu ochrony fizycznej;
- możliwość napadu przez zorganizowane grupy przestępcze | terrorystyczne,
- działające w sposób profesjonalny, przemyślany i zorganizowany;
- możliwość napadu przez pojedynczych przestępców lub przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w zakresle ochrony mienia w budynku AGH-D17

4.2. Symptomy mogące świadczyć o przygotowaniu napadu lub włamaniu do budynku

- wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami strefy II lub Pełnomocnika ds. Ochrony Informacji Niejawnych objawiające się m.in.: podejmowaniem prób pozyskiwania informacji o danym obiekcie, w pomieszczeniu od pracowników podczas luźnych rozmów po „przypadkowym" spotkaniu;
- nawiązanie rozmów przez osoby postronne z pracownikami AGH-D17
- podszywaniem się pod byłych pracowników budynku AGH-D17 i przejawianle zainteresowania tym, co się po latach zmieniło;
- interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych;
- obserwacja sposobu działania systemu ochronnego, sprzątania itp.;
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych;
- celowe uszkadzanie urządzeń alarmowych, linli telefonicznych, oświetlenia itp.;
- próby pozyskania do grup przestępczych, pracowników AGH-D17 (dotyczy głównie osób mające problemy finansowe, towarzyskie, a także służbowe).

4.3. Procedury postępowania z zagrożeniami zewnętrznymi

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzając ewentualne możliwości zaistnienia zagrożeń:

- systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację;

- stosować zasadę niedopuszczania osób niepowołanych do penetracji stref bezpieczeństwa;
- wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych.

4.4. Zagrożenia wewnętrzne

Zagrożeniami wewnętrznymi mogą być:

- nleznajomość lub ignorowanie przepisów w zakresie wykonywania, przechowywania i przetwarzania informacji niejawnych przez pracowników do tego upoważnionych;
- próby zaboru dokumentów lub mienia przez obecnych lub byłych pracowników;
- próby powielania, kserowania dokumentów służbowych dla celów prywatnych;
- rozpoznanie organizacji pracy celem łatwiejszej pracy grup przestępczych;
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione;
- nadmierne spożywanie alkoholu - przesłanką do wykroczeń dyscyplinarnych

4.5. Procedury postępowania z zagrożeniami wewnętrznymi

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzając ewentualne możliwości zaistnienia zagrożeń:

- zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu;
- prowadzić szczególny nadzór, by nie dokonywano prób kserowania, kopiowania bez nadzoru przełożonych

- uwrażliwienie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych;
- zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie wydane przez kierownika jednostki;
- wprowadzenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożycie alkoholu

5. Procedury działania osób odpowiedzialnych za ochronę informacji niejawnych w sytuacji szczególnych

5.1. Zasady postępowania w sytuacjach szczególnych

5.1.1. Nieplanowana nieobecność

Nieplanowana nieobecność Pełnomocnika Ochrony oraz pozostałych pracowników pionu ochrony informacji niejawnych AGH-D17. W przypadku nieplanowanej nieobecności Inspektora ds. Ochrony Informacji Niejawnych oraz pozostałych pracowników pionu ochrony Informacji niejawnych (gdy istnieje pilna potrzeba dostępu do dokumentów niejawnych) Prodziekan powołuje komisję, która pobiera od Prezydenta klucze zapasowe do pomieszczenia Pełnomocnika Ochrony, Kancelarii Materiałów Niejawnych i szafy metalowej. W skład komisji (minimum 3 osoby) mogą wchodzić tylko pracownicy AGH posiadający dopuszczenie do pracy z informacjami niejawnymi. Udostępnienie odpowiednich dokumentów upoważnionym osobom powinno się odbyć w Kancelarii Materiałów Niejawnych. Następnie komisja zamyka dokumenty w szafie stalowej, klucze zapasowe oddając do sejfu. Komisja sporządza protokół z otwarcia Kancelarii Materiałów Niejawnych, w którym wyszczególnia:

- skład komisji,
- cel otwarcia i na podstawie jakiej decyzji dokonano otwarcia, z jakich dokumentów korzystano,
- kto korzystał z tych dokumentów,
- datę i godzinę otwarcia i zamknięcia KMN, komu przekazano klucze.

5.1.2. Włamanie do Kancelarii Materiałów Niejawnych

W przypadku włamania się do KMN (szafy stalowej) Inspektor ds. Ochrony Informacji Niejawych powołuje komisję, która pobiera od Inspektora klucze zapasowe do KMN. W skład komisji (minimum 3 osoby) mogą wchodzić tylko osoby posiadający dopuszczenie do pracy z informacjami niejawnymi. Komisja przeprowadza spis natury dokumentów i materiałów niejawnych zastanych w KMN I sprawdza, czy stan faktycznych dokumentów niejawnych jest zgodny ze stanem ewidencyjnym (jeżeli jest taka możliwość). Następnie komisja sporządza protokół, w którym wyszczególnia:

skład komisji,

- cel otwarcia i na podstawie jakiej decyzji dokonano otwarcia, z jakich dokumentów korzystano,
- kto korzystał z tych dokumentów,
- datę i godzinę otwarcia i zamknięcia KMN, komu przekazano klucze.

5.2. Zasady postępowania w sytuacjach nadzwyczajnych

Rozróżnia się następujące stany nadzwyczajne:

- stan klęski żywiołowej;
- stan wyjątkowy
- stan kryzysu;
- stan wojny.

W sytuacjach nadzwyczajnych, gdy wzrasta zagrożenie dla przechowywanych dokumentów i materiałów niejawnych wzmacnia się ochronę II I III strefy ochronnej. Wzmocnienie ochrony Informacji niejawnych i aktualizacja dokumentacji (związane z przygotowaniem KMN

do ewakuacji) wprowadzane jest na zarządzenie Inspektora ds. Ochrony Informacji Niejawnych zgodnie z kartami realizacji zadań operacyjnych" umieszczonych w „Planie operacyjnym funkcjonowania miasta Krakowa w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny". Karty realizacji zadań operacyjnych obejmują osoby odpowiedzialne za przetwarzanie i ochronę Informacji niejawnych oraz wszystkie dokumenty niejawne.

Postępowanie w stanach nadzwyczajnych - jako stany nadzwyczajne uważa się stany określone w art. 228 Konstytucji RP (Dz.U.1997r. nr 78 poz.484 z póź.zm.) tj. stan wojenny, stan wyjątkowy lub stan klęski żywiołowej):

- wprowadza się dodatkowe obostrzenia i regulacje w zakresie fizycznej ochrony Kancelarii Materiałów Niejawnych;
- zaostrza się kontrolę osób wchodzących do budynku;
- sprawdza się funkcjonowanie sytemu alarmowego;
- archiwizuje się i zabezpiecza zawartość systemów teleinformatycznych;
- przeprowadza się naradę sposobami związanymi z dostępem do informacji niejawnych i udziela im się stosownego instruktażu w zakresie postępowania z dokumentami niejawnymi po wprowadzeniu stanu nadzwyczajnego;
- gromadzi się wszystkie dokumenty niejawne w Kancelarii Materiałów Niejawnych;
- przygotowuje się worki ewakuacyjne i protokoły przekazania zgromadzonych dokumentów i materiałów niejawnych;
- osiąga się gotowość do ewakuacji Kancelarii Materiałów Niejawnych.

Interesanci mogą wejść na teren budynku po okazaniu dowodu tożsamości, spisaniu danych osobowych oraz sprawdzaniu toreb (teczek).

W sytuacjach, gdy Rzeczpospolita Polska znajduję się w stanie wojny, wprowadzono stan wojenny, występuje realne zagrożenie grup terrorystycznych czy przestępczych albo też służb specjalnych państw obcych, oprócz wyżej opisanej wzmocnionej ochrony obiektu, osoby odpowiedzialne bezpośrednio za ochronę stref bezpieczeństwa realizują swoje zadania poprzez:

- wzmożenie czujności w ochronie strefy bezpleczeństwa, a zwłaszcza podczas wchodzenia do tej strefy interesantów;
- utrzymanie stałego kontaktu Inspektora ds. Ochrony Informacji Niejawnych ze służbą ochrony;
- systematyczne (codzienne) sprawdzanie kompleksowe systemów bezpieczeństwa m.in. kamer i drzwi.
- utrzymanie stałej gotowości do ewakuacji dokumentów z KMN.

5.3. Warianty ewakuacji Kancelarii Materiałów Niejawnych

Wariant zasadniczy:

W zależności od charakteru i rozmiaru zagrożenia stosować się będzie różne warianty ewakuacji. Decyzję o ewakuowaniu KMN podejmuje Prezydent Miasta Konina. Koordynatorem ewakuacji jest Pełnomocnik Ochrony, który współpracuje w tym zakresie z kierownikami jednostek i komórek organizacyjnych. Do ewakuacji wykorzystywać się będzie niepalne worki, plombowane po wypełnieniu dokumentami.

Niezależnie od wariantu, ewakuację prowadzi się w określonej kolejności:

1. dokumenty i materiały o najwyższych klauzulach tajności, urządzenia ewidencyjne I pieczęcie;
2. dokumenty I materiały o klauzulach „poufne” i „zastrzeżone";

6. Ustalenia końcowe

Przełożeni pracowników, a także Pełnomocnik ochrony:

- zapoznają podległych pracowników z ustaleniami Planu ochrony informacji niejawnych w Urzędzie,
- zapewnią bieżące przestrzeganie postanowień Planu ochrony w zakresie ochrony informacji niejawnych, mogących występować w działalności kierowanej komórki organizacyjnej.

W przypadku wystąpienia wątpliwości, a także potrzeby przybliżenia zasad dotyczących realizacji zadań związanych z ochroną informacji niejawnych, sporządzania i wykonania dokumentów zawierających informacje niejawne, pracownicy Urzędu mogą w każdym czasie zwracać się o wyjaśnienia czy też instruktaż do Pełnomocnika ochrony.

O wszelkich nieprawidłowościach, będących następstwem naruszenia zasad określonych w Planie ochrony, każdy pracownik jest zobowiązany niezwłocznie poinformować o tym swojego przełożonego, a ten Pełnomocnika ochrony, który podejmie stosowne działania zmierzające do wyjaśnienia okoliczności powstałej sytuacji.

W sprawach nieuregulowanych w planie ochrony mają zastosowanie odpowiednie przepisy ustawy o ochronie informacji niejawnych, aktów wykonawczych wydanych na jej podstawie oraz odpowiednich zarządzeń.

Plan ochrony informacji niejawnych podlega regularnej aktualizacji zgodnie z obowiązującymi przepisami prawa.

Dokument wchodzi w życie z dniem zatwierdzenia przez upoważnione osoby i pozostaje w mocy do czasu jego uchylenia lub zastąpienia nowym planem.

7. Załączniki

Załącznik nr. 1

Wzór upoważnienia do przetwarzania informacji o klauzuli „Zastrzeżone"

Miejscowość, data …….

Upoważnienie nr ……

Na podstawie art.21 ust.4 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. z 2019 r., poz. 742)

Upoważniam

Pana/Panią ……

Zatrudniony(a) ...……

PESEL ..……..

Imię ojca ……

Nazwa jednostki organizacyjnej ……..

Do dostępu do informacji niejawnych oznaczonych klauzulą „Zastrzeżone”

Niniejsze upoważnienie wydane jest na czas: ……

Pieczątka i podpis ..……

Załącznik nr. 2

WNIOSEK O PRZEPROWADZENIE POSTĘPOWANIA SPRAWDZAJĄCEGO

Na podstawie art. 23 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, wnoszę o przeprowadzenie postępowania sprawdzającego wobec niżej wymienionej osoby celem wydania poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych.

Dane osoby poddawanej postępowaniu sprawdzającemu:

Imię i nazwisko: .....

Data i miejsce urodzenia: .....

Obywatelstwo: .....

Numer PESEL: .....

Adres zamieszkania: .....

Stanowisko lub funkcja: .....

Poziom dostępu do informacji niejawnych: (np. ŚCIŚLE TAJNE, TAJNE, POUFNE)

W związku z powyższym uprzejmie proszę o wszczęcie postępowania sprawdzającego i wydanie stosownego poświadczenia bezpieczeństwa.

Z poważaniem,

……..

Załącznik nr. 3

Wzór zaświadczenia stwierdzającego odbycie szkolenia w zakresie ochrony informacji niejawnych

Zaświadczenie nr ……..

Stwierdza się, że Pan/Pani:

Imię i nazwisko: .....

Data i miejsce urodzenia: .....

Obywatelstwo: .....

Numer PESEL: .....

Odbyt/a* szkolenie w zakresie ochrony informacji niejawnych na podstawie przepisów ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (t. j. Dz.U. 2019 r. poz.742), zorganizowane przez Pelnomocnika ds. Ochrony Informacji Niejawnych.

Miejscowość, data ……

Pieczątka i podpis ..……

Załącznik nr. 4

Wykaz osób, które zapoznały się z „Planem ochrony informacji niejawnych" w Wydziale Informatyki

Imię	Nazwisko	Data	Podpis
