Załącznik nr 2
do Zarządzenia Nr 72/0101/2016 Rektora AJP
z dnia 7 listopada 2016 r.

Z A T W I E R D Z A M

Rektor AJP: *prof. dr hab. Elżbieta Skorupska-Raczyńska*

(Rektor Akademii im. Jakuba z Paradyża)

I N S T R U K C J A

dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli *zastrzeżone* w Akademii im. Jakuba z Paradyża oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony

Rozdział I.
Definicje
§ 1.

Użyte w Instrukcji określenia oznaczają:

1) ustawa – ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2016 r. poz. 1167),
2) AJP – Akademia im. Jakuba z Paradyża,
3) kierownik jednostki – Rektor Akademii im. Jakuba z Paradyża,
4) pełnomocnik – pełnomocnik ds. ochrony informacji niejawnych tj. osoba odpowiedzialna za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych podlegająca bezpośrednio Rektorowi Akademii im. Jakuba z Paradyża,
5) Kancelaria Informacji Niejawnych – miejsce przetwarzania i przechowywania dokumentów niejawnych,
6) przetwarzanie informacji niejawnych – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie,
7) wykonawca – pracownik zajmujący określone stanowisko służbowe, wykonujący zadania zgodnie z zakresem obowiązków, posiadający stosowne poświadczenie bezpieczeństwa lub upoważnienie oraz przeszkolenie w zakresie ochrony informacji niejawnych,
8) rękojmia zachowania tajemnicy – zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego,
9) dokument – każda utrwalona informacja niejawna,
10) materiał – dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna,

11) przesyłka – materiały w postaci odpowiednio zabezpieczonych, zaadresowanych i oznaczonych paczek lub listów,
12) rejestr ewidencyjny – księga, dziennik, wykaz, spis, rejestr lub kartoteka o ustalonych rubrykach, prowadzona w formie papierowej lub elektronicznej, służąca do rejestrowania dokumentów zawierających informacje niejawne oraz umożliwiająca kontrolę ich stanu i obiegu.

Rozdział II.
Zakres przedmiotowy i podmiotowy
§ 2.

1. Informacje niejawne stanowiące tajemnicę w AJP oznaczone klauzulą *zastrzeżone* dotyczą:
   1) danych o zakresie zadań obronnych Ministra Nauki i Szkolnictwa Wyższego oraz AJP,
   2) wybranych danych dotyczących spraw personalnych kadry kierowniczej AJP, współpracy AJP z instytucjami wojskowymi w zakresie obronności,
   3) Stałego Dyżuru w AJP w czasie stanu zagrożenia państwa,
   4) danych dotyczących spraw mobilizacyjnych,
   5) ochrony dokumentów niejawnych,
   6) funkcjonowania kancelarii niejawnej w czasie stanu zagrożenia państwa,
   7) informacji dotyczących ujawnienia informacji niejawnych,
   8) danych dotyczących systemów teleinformatycznych w przetwarzaniu informacji niejawnych,
   9) haseł i kodów dostępu do urządzeń komputerowych zawierających informacje niejawne oznaczone klauzula *zastrzeżone,*
   10) dokumentów dotyczących postępowania sprawdzającego w związku z upoważnieniem pracowników do informacji niejawnych,
   11) szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji systemów i sieci teleinformatycznych służących do wytwarzania, przetwarzania, przekazywania lub przechowywania informacji oznaczonych klauzulą zastrzeżone,
   12) planów realizacji zadań związanych z osiąganiem podwyższonej i pełnej gotowości obronnej państwa przypisanych AJP,
   13) zarządzeń Rektora w sprawie opracowywania dokumentów i planów funkcjonowania w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i wojny.
2. Wykaz stanowisk pracy w AJP, z którymi może łączyć się dostęp do informacji niejawnych:
   1) objętych klauzulą *poufne:*
      a) Rektor,
      b) Pełnomocnik,
   2) objętych klauzulą *zastrzeżone:*
      a) prorektorzy,
      b) dziekani i ich zastępcy,
      c) kanclerz i jego zastępcy,
      d) kwestor i jego zastępca,
      e) kierownik Działu Organizacyjno-Prawnego i Kadr,

f) radcy prawni,
g) kierownik Kancelarii Informacji Niejawnych,
h) inspektor bezpieczeństwa teleinformatycznego,
i) administrator Systemu Bezpieczeństwa Teleinformatycznego,
j) dyrektor Biblioteki Głównej im. Elizy Orzeszkowej,
k) samodzielne stanowisko ds. zamówień publicznych,
l) pracownicy AJP wytypowani do pełnienia służby w ramach Stałego Dyżuru AJP.

Rozdział III.
Zasady przetwarzania materiałów niejawnych o klauzuli *zastrzeżone*
§ 3.

1. Informacjom niejawnym nadaje się klauzulę *zastrzeżone,* jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez AJP zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.
2. Dokumenty opatrzone klauzulą *zastrzeżone* oznacza się zgodnie z zasadami określonymi w odpowiednim akcie wykonawczym – obecnie w rozporządzeniu Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczenia materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288, poz.1692).
3. Klauzule *zastrzeżone* nadaje Rektor lub osoba, która jest przez niego upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
4. Informacje niejawne oznaczone klauzulą *zastrzeżone* mogą przetwarzać (wytwarzać, modyfikować, kopiować, przechowywać, klasyfikować, przekazywać lub udostępniać) osoby, które:
   1) posiadają pisemne upoważnienie Rektora uprawniające do dostępu do informacji niejawnych o klauzuli *zastrzeżone* lub posiadają poświadczenie bezpieczeństwa osobowego,
   2) oraz odbyły szkolenie w zakresie ochrony informacji niejawnych i uzyskały stosowne zaświadczenie,
   3) oraz są ujęte w *Wykazie osób zatrudnionych w AJP, które posiadają uprawnienia do dostępu do informacji niejawnych.*
5. Dokumenty oznaczone klauzula *zastrzeżone* mogą być wytwarzane metodą ręcznego pisania, maszynopisania lub w postaci plików elektronicznych – w pomieszczeniach służbowych zapewniających wymagane przepisami warunki ochrony informacji niejawnych, w sposób uniemożliwiający ich nieuprawnione ujawnienie.
6. Komputery, w których przetwarzane są dokumenty oznaczone klauzulą *zastrzeżone* muszą być odseparowane fizycznie od sieci jawnych, w tym zwłaszcza sieci ogólnie dostępnych, w szczególności od Internetu. Wykonanie tego warunku nadzoruje inspektor bezpieczeństwa teleinformatycznego.
7. Wersje robocze dokumentów niejawnych należy wykonywać w zarejestrowanych w kancelarii niejawnej brudnopisach, na nośnikach magnetycznych lub na niezapisanych stronach sporządzanego dokumentu, oznaczonych klauzulą co najmniej równa klauzuli wykonywanego materiału.

8. Dokumenty oznaczone klauzulą *zastrzeżone* należy sporządzać w ściśle określonej liczbie egzemplarzy i rozsyłać do adresatów na podstawie rozdzielnika uzgodnionego z Rektorem.
9. Liczbę wytwarzanych dokumentów oraz zasięg ich obiegu ogranicza się do minimum niezbędnego do realizacji zadań służbowych, w miarę możliwości wykorzystując inne możliwości załatwienia tematu.
10. Wykonanie kopii, odpisu, wypisu, wyciągu może nastąpi za zgodą Rektora lub Pełnomocnika, o ile wykonawca dokumentu nie dokonał zastrzeżenia w tym zakresie.
11. Wykonanie kopii, odpisu, wyciągu, tłumaczenia odnotowuje się na dokumencie, z którego kopię, odpis, wyciąg, tłumaczenie wykonano, zamieszczając informacje o:
    1) nazwie komórki administracyjnej lub jednostki organizacyjnej, w której wykonano kopię, odpis, wyciąg lub tłumaczenia,
    2) liczbie wykonanych egzemplarzy i adresatach,
    3) dacie sporządzenia kopii, odpisów, wyciągów lub tłumaczeń,
    4) numerze, pod jakim wykonany dokument został zarejestrowany w Dzienniku ewidencji (Dziennik ewidencji dla dokumentów wykonywanych techniką ksero jest w dyspozycji Pełnomocnika).
12. Informacje wyszczególnione w ust. 11 pkt 1-3 nanosi się na oryginale dokumentu przed wykonaniem kopii, odpisu, wyciągu, tłumaczenia.
13. Numer, pod jakim dokument został zarejestrowany, o którym mowa w ust. 11 pkt 4, nanosi się na oryginale dokumenty po jego wykonaniu.
14. Informacje, o których mowa w ust. 11 potwierdza się czytelnym podpisem osoby wykonującej kopię, odpis, wyciąg, tłumaczenie.
15. Zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu potwierdza na podstawie upoważnienie Rektora – Pełnomocnik.
16. Informacje zawarte w dokumentach oznaczonych klauzulą zastrzeżone podlegają ochronie przez okres określony przez wykonawcę do daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności, o ile Rektor nie przedłużył tego czasu lub nie określił czasu krótszego.

Rozdział IV.
Udostępnianie dokumentów niejawnych oznaczonych klauzulą *zastrzeżone*
§ 4.

1. Informacje niejawne oznaczone klauzulą *zastrzeżone* mogą być udostępniane wyłącznie osobom upoważnionym pisemnie przez Rektora lub posiadającym poświadczenia bezpieczeństwa uprawniające co najmniej do dostępu do wiadomości oznaczonych klauzulą *zastrzeżone,* przeszkolonym z przepisów o ochronie informacji niejawnych i tylko w zakresie niezbędnym do wykonywania obowiązków na zajmowanym stanowisku służbowym.
2. Udostępnienie w/w informacji wytworzonych w komórkach administracyjnych lub jednostkach organizacyjnych AJP określonej osobie lub instytucji może nastąpić tylko na podstawie pisemnej zgody Rektora lub upoważnionej przez niego osoby. Zgoda powinna określać zakres podmiotowy i przedmiotowy udostępnienia informacji. Zgoda nie oznacza zmiany lub zniesienia klauzuli tajności.
3. Przekazywanie dokumentów niejawnych oznaczonych klauzulą *zastrzeżone* poza teren AJP realizuje się wyłącznie za pośrednictwem Pełnomocnika, na zasadach określonych w odrębnych przepisach – zgodnie z rozporządzeniem Rady Ministrów z dnia 7 grudnia

2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. Nr 276, poz. 1631 ze zm.).

4. Osoby, które zapoznały się z informacjami niejawnymi oznaczonymi klauzulą *zastrzeżone,* są zobowiązane do:
    1) nie ujawniania tych informacji osobom nieuprawnionym, także po rozwiązaniu umowy o pracę lub po przejściu a emeryturę, rentę,
    2) nie przekazywania ich przez nieutajnione środki łączności,
    3) nie wykorzystywania informacji niejawnych oznaczonych klauzulą *zastrzeżone* wytworzonych, przechowywanych i przetwarzanych w komórkach administracyjnych lub jednostkach organizacyjnych AJP na wykładach, referatach, publikacjach i innych wystąpieniach publicznych oraz w indywidualnej twórczości naukowej i publicystycznej.
5. Dopuszcza się czasowe przekazywanie dokumentów oznaczonych klauzulą *zastrzeżone* pomiędzy wykonawcami z tej samej komórki administracyjnej lub jednostki organizacyjnej. Może ono nastąpić z pominięciem kancelarii niejawnej, za pokwitowaniem.
6. O utracie dokumentów niejawnych i wszelkich innych zjawiskach zagrażających bezpieczeństwu informacji o klauzuli *zastrzeżone* pracownicy AJP są zobowiązani do niezwłocznego powiadamiania swoich przełożonych, Rektora i Pełnomocnika.

Rozdział V.
Zasady postępowania z otrzymaną dokumentacją niejawną obowiązujące w Rektoracie AJP
§ 5.

1. Przesyłka niejawna posiada na kopercie następujące dane:
    1) klauzulę tajności (zastrzeżone) lub dodatkowe oznaczenie (do rąk własnych),
    2) imienne określenie adresata,
    3) imię i nazwisko osoby pakującej/kopertującej, a miejsca sklejania koperty opieczętowane są pieczęcią *do pakietów* i zaklejone taśma samoprzylepną.
2. Zewnętrzna korespondencja niejawna o klauzuli *zastrzeżone* odbierana jest przez Kancelarię Ogólną.
3. Kancelaria Ogólna przekazuje przesyłkę w nienaruszonej kopercie pracownikowi Rektoratu AJP posiadającemu uprawnienie do dostępu do informacji niejawnych, za pokwitowaniem.
4. Po otrzymaniu przesyłki uprawniony pracownik sekretariatu:
    1) sprawdza czy sposób pakowania jest zgodny z powyższym opisem,
    2) sprawdza czy przesyłka jest nienaruszona,
    3) powiadamia Pełnomocnika, który osobiście odbiera przesyłkę, także tą z adnotacją *do rąk własnych.*
5. Dalszy obieg przesyłki niejawnej odbywa się poprzez Kancelarie Informacji Niejawnych.

Rozdział VI.
Zasady ewidencjonowania, przekazywania, kompletowania i niszczenia dokumentów oznaczonych klauzulą *zastrzeżone*
§ 6.

1. Dokumenty wytworzone w AJP, zawierające informacje niejawne o klauzuli *zastrzeżone,* ewidencjonuje kierownik Kancelarii Informacji Niejawnych w Dzienniku ewidencji.
2. Dokument dodatkowo wytworzony (kopia, wyciąg, odpis) ewidencjonuje się każdorazowo pod oddzielną pozycją w Dzienniku ewidencji.
3. Dopuszcza się rejestrowanie w jednym dzienniku dokumentów otrzymanych i wysłanych.
4. Dokumenty opatrzone klauzulą *zastrzeżone,* oznacza się zgodnie z zasadami określonymi w odrębnych przepisach – rozporządzenie prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczenia materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288, poz.1692).
5. Przekazywanie dokumentów oznaczonych klauzule *zastrzeżone* innym komórkom administracyjnym lub jednostkom organizacyjnym może nastąpić wyłączni za pośrednictwem Kancelarii Informacji Niejawnych na zasadach określonych odrębnie – rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. Nr 276, poz. 1631 ze zm.).
6. Kancelaria Informacji Niejawnych udostępnia dokumenty niejawne oznaczone klauzulą *zastrzeżone* wyłącznie wykonawcom posiadającym pisemne upoważnienie Rektora lub poświadczeniem bezpieczeństwa osobowego i zaświadczenie o przeszkoleniu z zasad ochrony informacji niejawnych, za podpisem we właściwym urządzeniu ewidencyjnym. W przypadku, kiedy pobierający dokument niejawny nie ma możliwości właściwego jego zabezpieczenia, zapoznaje się z jego treścią w pomieszczeniu Kancelarii Informacji Niejawnych.
7. Dokumenty oznaczone klauzulą *zastrzeżone*, wytworzone w komórce administracyjnej lub jednostce organizacyjnej oraz otrzymane od innych komórek i jednostek, po ich wykorzystaniu należy przekazać do Kancelarii Informacji Niejawnych, w której podlegają:
    1) skompletowaniu w teczki akt lub segregatory, jeżeli stanowią wartość praktyczną dla AJP,
    2) zwrotowi do nadawcy, jeżeli określił on taki sposób postępowania z przesłanymi materiałami,
    3) bieżącemu niszczeniu, jeżeli dokument nie posiada wartości użytkowej lub archiwalnej.
8. Niearchiwalne dokumenty oznaczone klauzulą *zastrzeżone* niszczy się protokolarnie sporządzając *Protokół zniszczenia dokumentów niejawnych.*
9. Niszczenia protokolarnego dokonuje komisja powołana przez Rektora.
10. Członkowie komisji musza posiadać co najmniej pisemne Upoważnienie do dostępu do informacji niejawnych oznaczonych klauzulą *zastrzeżone* wydane przez Rektora lub odpowiednie poświadczenie bezpieczeństwa osobowego oraz odbyli szkolenie w zakresie ochrony informacji niejawnych.
11. Na podstawie *Protokołu zniszczenia dokumentów niejawnych* Pełnomocnik zdejmuje wyszczególnione w nim dokumenty z ewidencji poprzez naniesienie w rubryce *Adnotacje o zniszczeniu* odpowiedniego rejestru ewidencyjnego adnotację o treści

protokół zniszczenia nr …. z dnia …poz. Nr…. oraz uwierzytelnia wpis wpisaniem daty, podpisem i pieczątką.

Rozdział VII.
Zasady ochrony fizycznej dokumentów zawierających informacje niejawne oznaczone klauzulą zastrzeżone
§ 7.

1. Dokumenty oznaczone klauzulą *zastrzeżone* przechowuje się co najmniej w szafach lub w szufladach biurka zamykanych na klucz, w Kancelarii Informacji Niejawnych lub pomieszczeniach służbowych wykonawców lub upoważnionych użytkowników, w sposób uniemożliwiający ich nieuprawnione ujawnienie. Dotyczy to także sytuacji czasowego opuszczania pomieszczeń służbowych w godzinach pracy.
2. Dokumenty oznaczone klauzulą *zastrzeżone* oraz dokumenty jawne należy przechowywać oddzielnie.
3. Materiały o różnych klauzulach tajności, a także jawne mogą być przechowywane wspólnie, jeżeli dotyczą jednej, tej samej sprawy.
4. Wykonawca odpowiada za właściwe zabezpieczenie posiadanych dokumentów.
5. Każdorazowo, po zakończeniu godzin pracy, wykonawcy mają obowiązek zabezpieczenia posiadanych dokumentów i materiałów oznaczonych klauzulą *zastrzeżone* w sposób określony w ust. 1. Wykonawcy nieposiadający urządzeń, o których mowa w ust.1, przekazują posiadane materiały do Kancelarii Informacji Niejawnych.
6. Klucze do pomieszczeń przechowuje się w sposób określony w Planie ochrony informacji niejawnych w AJP.
7. Pod nieobecność wykonawców dokumentów niejawnych oznaczonych klauzulą *zastrzeżone:*
    1) urządzenia, w których przechowywane są te dokumenty, może otworzyć za zgodą jego bezpośredniego przełożonego komisja powołana przez Rektora składająca się z co najmniej trzech osób, w tym Pełnomocnika, przy czym wszyscy członkowie komisji muszą posiadać upoważnienia Rektora do dostępu do informacji niejawnych o klauzuli *zastrzeżone* lub poświadczenia bezpieczeństwa osobowego,
    2) komisja sporządza i przekazuje do Kancelarii Informacji Niejawnych protokół z podjętych czynności, który powinien zawierać:
        a) datę dokonania czynności,
        b) wyliczenie numerów ewidencyjnych pobranych dokumentów oraz wskazanie osoby, której materiał przekazano,
        c) podpisy członków komisji.
8. W przypadku wyjazdu służbowego, oddelegowania do wykonywania zadań służbowych poza miejscem pracy lub urlopu trwającego powyżej jednego miesiąca, wykonawca ma obowiązek przekazania za podpisem posiadane dokumenty oznaczone klauzulą *zastrzeżone* osobie, która będzie posiadała dostęp do informacji niejawnych oraz będzie wykonywała obowiązki podczas jego nieobecności.
9. O sposobie przewozu materiałów niejawnych oznaczonych klauzulą *zastrzeżone* decyduje Pełnomocnik w porozumieniu z Rektorem, zgodnie z odrębnymi przepisami – rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 271, poz. 1603).

10. Zabrania się:
    1) wynoszenia dokumentów oznaczonych klauzulą *zastrzeżone,* urządzeń, nośników na których zarejestrowano ten dokument poza strefę uniemożliwiającą ich nieuprawnione ujawnienie bez zgody Pełnomocnika ds. ochrony informacji niejawnych i ich należytego zabezpieczenia przed dostępem osób nieuprawnionych,
    2) przekazywania i udostępniania informacji niejawnych, wiadomości dotyczących wykonywanej pracy oraz przedsięwzięć i spraw służbowych osobom nieuprawnionym,
    3) sporządzania notatek zawierających wiadomości niejawne w nie ewidencjonowanych nośnikach informacji (notatnikach, dyskietkach, zeszytach, itp.).
11. Wszelkie nieprawidłowości związane z naruszeniem zasad, o których mowa w niniejszym Rozdziale należy niezwłocznie zgłaszać Pełnomocnikowi.

Rozdział VIII.
Postępowanie w przypadku naruszenia zasad ochrony lub ujawnienia informacji niejawnych oznaczonych klauzulą *zastrzeżone*
§ 8.

1. Kierownicy komórek administracyjnych lub jednostek organizacyjnych AJP mają obowiązek powiadomić Pełnomocnika i Rektora o każdym stwierdzonym fakcie:
    1) naruszenia bezpieczeństwa informacji oznaczonych klauzulą *zastrzeżone,* polegającym na zaniechaniu właściwego działania lub działaniu niezgodnym z przepisami o ochronie informacji niejawnych, mogącym spowodować ujawnienie tych informacji,
    2) ujawnienia informacji o utracie, zagubieniu, kradzieży dokumenty lub innego przedmiotu niejawnego albo udostępnieniu go osobie nieupoważnionej.
2. W przypadkach opisanych wyżej Pełnomocnik w porozumieniu z Rektorem podejmuje niezwłocznie działania zmierzające do:
    1) wyjaśnienia okoliczności naruszenia przepisów i ustalenia osób winnych tych naruszeń,
    2) określenia stopnia szkody z tym związanej,
    3) zminimalizowanie skutków powstałych szkód,
    4) podjęcia przedsięwzięć prewencyjnych.
3. Wyniki postępowania wyjaśniającego, o którym mowa w ust. 2, Pełnomocnik przestawia Rektorowi, który decyduje o wyciągnięciu konsekwencji służbowych wobec winnych. W stosunku do osób posiadających pisemne upoważnienie do dostępu do informacji niejawnych o klauzuli *zastrzeżone*, które w sposób rażący naruszyły przepisy o ochronie informacji niejawnych Pełnomocnik lub ABW przeprowadzają kontrolne postępowanie sprawdzające, z pominięciem terminów określonych w art. 33 ust. 9-10 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2016 r. poz. 1167) i obowiązku wypełniania nowej ankiety bezpieczeństwa przez osobę sprawdzaną.

Rozdział IX.
ODPOWIEDZIALNOSC KARNA I DYSCYPLINARNA
§ 9.

Na podstawie ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (t.j. Dz. U. z 2016 r. poz. 1137 ze zm.) pracowników AJP obowiązują następujące przepisy dotyczące przestępstw przeciwko ochronie informacji:

1) **Art. 266:**
   a) **§ 1.** Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
   b) **§ 2.** Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli *zastrzeżone* lub *poufne* lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.
   c) **§ 3.** Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.
2) **Art. 267. § 1.** Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
3) **Art. 268:**
   a) **§ 1.** Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
   b) **§ 2.** Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
   c) **§ 3.** Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
4) **Art. 269:**
   a) **§ 1.** Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
   b) **§ 2.** Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

§ 10.

Na podstawie Art. 100 § 2 ustawy z dnia 26 czerwca 1974 roku Kodeks Pracy (tj. Dz. U. z 2016 poz. 1666 ze zm.) pracownik jest zobowiązany m.in. do *zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę oraz do przestrzegania tajemnicy określonej w odrębnych przepisach.* Za naruszenie w/w przepisów kierownik jednostki organizacyjnej ma prawo zastosować jedną z poniższych kar:

1) karę upomnienia,
2) karę nagany,
3) karę pieniężną.

Rozdział X.
Postanowienia końcowe

§ 11.

W sprawach nieuregulowanych niniejszą Instrukcją, a związanych z przetwarzaniem informacji niejawnych o klauzuli *zastrzeżone* każdorazowo należy zasięgnąć opinii Pełnomocnika.