(ЛОГО-ФИРМА)	ПРОЦЕДУРА-ПОЛИТКА	(НУМЕРАЦИЈА)
Класиф.(ограничено…)		Верзија

ПОЛИТИКА КЛАСИФИКАЦИЈЕ ИНФОРМАЦИЈА

	Назив/име	позиција	датум
Усвојио	…	…	…
Одобрио	…	…	…
Направио	…	…	…
Власник/одговоран	*(Одељење)*		
Важи од			…
Примењује се на	…		

ИСТОРИЈА ДОКУМЕНТА

ВЕРЗИЈА	ДАТУМ	АУТОР	ОПИС	

САДРЖАЈ

1 РЕЗИМЕ 3

2 УВОДНЕ ОДРЕДБЕ 3

2.1 Сврха 3

2.2 Опис 3

2.3 Референце 3

3 ОПШТЕ ОДРЕДБЕ 4

3.1 Опсег 4

3.2 Дефиниције 4

4 ПОЛИТИКА 5

4.1 Опште одредбе 5

4.2 Политика 5

4.3 Улоге и одговорности 6

4.3.1 Власник информације – информационог добра 6

4.3.2 Старатељ информација 6

4.3.3 Корисник информација 7

5 ПРАВИЛА 7

5.1 Класификација информација 7

5.2 Правила руковања информацијом 9

6 ЗАВРШНЕ ОДРЕДБЕ 10

7 ПРИЛОЗИ 11

1 РЕЗИМЕ

Према регулаторним и захтевима Политике информационе безбедности <ИНСТИТУЦИЈЕ> неопходно је успоставити оквир за адекватан третман информационих добара. Сви запослени и уговорни спољни партнери морају бити упознати са релевантним и поступати сагласно томе.

2 УВОДНЕ ОДРЕДБЕ

2.1 Сврха

Сврха ове Политике јесте успостављање система категорисања информација у контексту захтева информационе безбедности и дефинисања релевантних правила за третман сваке од категорија како и се обезбедио одговарајући ниво заштите одн. поверљивости, интегритета и расположивости информације

2.2 Опис

Информациони систем <ИНСТИТУЦИЈЕ> мора имплементиране различите контроле у циљу умањивања ризика по ИКТ системе и/или контролисане податке.

Аспекти информационе безбедности на које се односи ова Политика укључују:

- поверљивост или значај информације у критичности последица уколико исте буду изгубљене или уништене због неодговарајућег третмана;
- немогућност адекватне заштите информација уколико иста није класификована на одговарајући начин у смислу специфицирања нивоа осетљивости или поверљивости;
- немогућност управљања самом информацијом и приступом уколико власништво и старатељство над информацијама није специфицирано за сваки сегмент.

2.3 Референце

- Политика информационе безбедности;
- Закон о информационој безбедности;
- Политика управљања ризицима;
- Анализа утицаја на пословање;
- План за континуитет пословања.

3 ОПШТЕ ОДРЕДБЕ

3.1 Опсег

Процедура се примењује на све запослене у <ИНСТИТУЦИЈИ>, уговорне спољне партнере који имају приступ информацијама < ИНСТИТУЦИЈЕ>, као и треће стране које су корисници и имају одговорност да познају и буду у сагласности са овом Политиком и свим законским и регулаторним актима и другим одредницама у области које су применљиве на њихове активности.

Сви наведени су у обавези да се увек придржавају актуелне верзије овог документа.

3.2 Дефиниције

- **информациона безбедност** - скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити тајност, интегритет, поверљивост, аутентичност и непорецивост тих података;
- **тајност** – својство које значи да податак није доступан неовлашћеним лицима;
- **интегритет** - очуваност изворног садржаја и целовитости податка;
- **расположивост** - својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
- **аутентичност** је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
- **непорецивост** - а способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
- **информациона добра -** обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и слично.
- **критични сервиси** – сервиси означени првим приоритетом у Анализи утицаја на пословање (*Business Impact Analysis, BIA*);
- **безбедносни инцидент** – било која активност која представља претњу по доступност, интегритет или поверљивост информационих добара, или био која активност која представља повреду политике информационе безбедности; покушај или успешни пробој имплементираних мера, неауторизовани приступ коришћење, откривање, модификација или уништење информација или уплитање у рад елемената одн. система у ИКТ систему.

4 ПОЛИТИКА

4.1 Опште одредбе

Сви запослени и треће стране које управљају информацијама у име < ИНСТИТУЦИЈЕ> имају личну одговорност да обезбеде примену одговарајућих безбедносних контрола на информације којима управљају. Одговарајуће безбедносне контроле могу се разликовати зависно од класификације информација, а примењују се правила руковања за релевантну категорију.

Додатне мере (контроле) примењују се на повезана информациона добра тако да буду сагласни захтевима и препорукама дефинисане категорије, регулативе, релевантних стандарда и добре праксе.

4.2 Политика

1. Све информације категоришу се сагласно правилима датим у одељку Класификација информација.
2. Ниво заштите процењује се на основу анализе тајности, интегритета и расположивости и свих других захтева који се разматрају у контексту информације и последица нарушавања информационе безбедности. Класификација и повезане заштитне контроле узимају у обзир пословну потребу за дељењем или рестрикцијом информација и последицама које су повезане са овим потребама
3. Власник информације је одговоран за одређивање вредности информације у ИКТ систему и доделу одговарајуће категорије; све информације које спадају у неку категорију означавају се на исти начин.
4. Информацијом се управља кроз њен циклус и иста може бити ре-класификована сагласно промени осетљивости и/или критичности.
5. Информацијом ће се руковати сагласно правилима датим у одељку Правила руковања информацијом.
6. Ако нека информација спада у више од једне категорије, примењује се виша (рестриктивнија) категорија
7. Уколико је трећа страна одговорна за управљање информацијом < ИНСТИТУЦИЈЕ>, иста је уговорно обавезна да се придржава ове Политике пре размене информација.
8. Уколико < ИНСТИТУЦИЈА> управља информацијама неке треће стране која има своју класификацију, писменом сагласношћу ће се одредити која правила се примењују пре размене тих информација.
9. Одговорност је сваког појединца који рукује информацијама покривеним овом Политиком да класификовани материјал адекватно означи, примени одговарајућа правила руковања за сваку категорију информација; уколико је потребно, савет за појашњење како означити или руковати одређеном информацијом затражиће од свог надређеног или од особе надлежне за координацију Информационе безбедности.

4.3 Улоге и одговорности

4.3.1 Власник информације – информационог добра

1. Информација коју процесира неки систем има додељеног власника. Ова одговорност се формално додељује и документује.
2. Власници информација су власници пословног процеса одн. руководиоци одељења којима је дато право да прикупљају, креирају, чувају и одржавају информације и информационе системе унутар области које су им поверене.
3. Власници информација могу делегирати неке оперативне одговорности, али задржавају одговорност.
4. Од Власника информација тражи се да:
   a) одреде вредност информације у информационом систему;
   b) одреде захтеве који се односе на приватност и чување информација;
   c) доделе одговарајућу ознаку класификације – у сагласности са Одељењем за регулаторна питања, Интерну ревизију и Информациону безбедност;
   d) доделе старатељство над информацијама;
   e) ауторизују приступ информацијама;
   f) специфицирају контроле које су потребне да би се очувала тајност, интегритет и расположивост;
   g) објаве ове захтеве за контролама Старатељима и Корисницима информација;
   h) припреме план за опоравак одн. континуитет за оне информације које су идентификоване
      i) као ризичне
      ii) виталне за пословање,
   - и саопште ово Старатељу информација.

4.3.2 Старатељ информација

1. Старатељи информација су појединци који контролишу информациони систем и без обзира на физичку или логичку локацију, медиј чувања, технологију у употреби или намену којој служе.
2. Старатељ информација одговоран је за администрирање контрола које специфицира Власник информација. Ово укључује
   a) Процену ефективности контрола у односу на потребна улагања, а према атрибутима класификације које је поставио Власник информација;
   b) Имплементацију физички и/или техничких контрола;
   c) Администрацију приступа информацијама;
   d) Обезбеђивање расположивости информација кроз имплементацију одговарајућих опција за опоравак сагласно критичности информација које су им у поседу, и то према плану за опоравак од катастрофалних догађаја или плану континуитета пословања који је припремио Власник информација.

4.3.3 Корисник информација

1. Корисник информација је појединац коме је експлицитно одобрено од стране Власника информација да приступа/мења/ брише /користи информацију у неком информационом систему.
2. Корисник информација одговоран је да :
   a) користи информацију само за намену коју јој је одредио Власник;
   b) буде у сагласности са свим контролама успостављеним од стране Власника и Старатеља;
   c) обезбеди да информација под неком класификацијом не буде откривена никоме ко за то нема одобрење Власника;
   d) уништава информације само на начин сагласан захтевима релевантне политике за чување и уништавање информација.

5 ПРАВИЛА

5.1 Класификација информација

КАТЕГОРИЈА	ниво последица	Опис	Пример
ЈАВНО	низак	Погодно за интерну и јавну дистрибуцију без последица по < ИНСТИТУЦИЈУ> одн. њене запослене и деоничаре. Класификација мора бити претходно одобрена пре употребе одн. означавања.	Маркетиншки материјал спремљен и одобрен за јавну употребу : рекламе, огласи, брошуре, каталози, изјаве за јавност, Интернет странице, годишњи прегледи, … Друге информације које регулатива захтева да буду јавно објављене.
ИНТЕРНО	умерен	Информације чија је доступност ограничена на неке запослене, партнере, добављаче или повезане ентитете. Размена изван дефинисаног круга била би непримерена. Доступ информацији изван дефинисаног круга одн. < ИНСТИТУЦИЈЕ> захтева одобрење управе.	Већина корпоративних докумената спада у ову категорију Интерни дописи, материјали за обуку, политике/процедуре/радне-инструкције/упутства, промотивни материјал пре званичног објављивања, трансакциони подаци, извештаји о продуктивности, уговори, Уговори о нивоу пружања услуга (SLA), подаци на интранету, интерни именик, ...
ПОВЕРЉИВО	висок	Информације осетљиве природе, под правном заштитом или високо вредне за < ИНСТИТУЦИЈУ> - компанијске или личне. Лични подаци, комерцијално или правно привилеговане информације, информације под ембаргом. Могу бити о појединцу или институцији. Не смеју бити доступне изван <	Лозинке и приступни креденцијали, токени за VPN приступ, подаци са платних картица, личне инфромације (нпр. матични бр., записи у кадровској служби, ...), истраживачко-развојјни подаци, већина књиговодствених података, друге осетљиве и високо вредне интерне информације.

ИНСТИТУЦИЈЕ> без експлицитног одобрења највишег нивоа управе.

5.2 Правила руковања информацијом

Категорија / *Контрола*	ЈАВНО	ИНТЕРНО	ПОВЕРЉИВО
Означавање	Не (опционо)	на свакој страници или у насловној линији е-поруке	на свакој страници или у насловној линији е-поруке
Умножавање	Није ограничено (уз поштовање ауторских права)	Ограничен број копија, уз претходно потписане уговоре о неоткривању	Ограничени број копија само уз претходно добијено одобрење овлашћене стране и регулисано "писаним" (одн. еквивалентим) путем.
Дистрибуција	Није ограничено (уз поштовање ауторских права)	Пошта: затворена адресирана препоручена пошиљка или курирском службом Телефакс: по упутству извора (оптимално у случају да је прималац на вези и поред апарата приликом слања). Е-пошта: само на проверену е-адресу примаоца, у случају слања изван < ИНСТИТУЦИЈЕ> енкриптована порука	Пошта: запечаћена пошиљка, лична испорука / курирска служба Телефакс: само уз непосредну потврду пријема тестне стране и примљене целе пошиљке. Е-пошта: само на проверену е-адресу примаоца, енкриптована порука и садржај прилога уз претходну размену кључева одвојеним каналом.
Чување	Нема посебних захтева	Физички материјал: Обезбеђена канцеларија или сл. (приступ просторији ограничен на запослене и овлашћене особе). Електронски облик: организовано у базама података или по фасцикалама и датотекама са контролисаним приступом (права, креденцијали)	Физички материјал: Уколико власник није пристуан, на сигурном месту "под кључем" Електронски облик: у базама података или фасциклама и датотеткама са контролисаним приступом (права, креденцијали) и у енкриптованом облику.
Уништавање	Стандардно одлагање смећа/рециклажа; ако постоји сумња у категоризацију, користити резач са сецкањем (cross-cut shredder) или др. решење сертификовано за безбедно уништавање. Медије унишавати одобреним средствима/методама тако да се обезбеди перманентно уништење података (shredding, физичко уништење; degauss за магнетне медије). Брисање података програмима и протоколом који је одредило Одељење за информациону безбедност.	Користити резач са сецкањем (cross-cut shredder) или др. решење сертификовано за безбедно уништавање. Медије унишавати одобреним средствима/методама тако да се обезбеди перманентно уништење података (shredding, физичко уништење; degauss за магнетне медије). Брисање података програмима и протоколом који је одредило Одељење за информациону безбедност.).	Користити резач са сецкањем (cross-cut shredder) или др. решење сертификовано за безбедно уништавање. Медије унишавати одобреним средствима/методама тако да се обезбеди перманентно уништење података (shredding, физичко уништење; degauss за магнетне медије). Брисање података програмима и протоколом који је одредило Одељење за информациону безбедност.).

6 ЗАВРШНЕ ОДРЕДБЕ

Повреде одредби из ове политике могу довести до примене дисциплинских мера према важећим интерним актима, сагласно степену повреде. Уколико је у повреду одредби укључена трећа страна, исте се могу сматрати повредом одредби уговора.

Политика ступа на снагу на дан усвајања.

7 ПРИЛОЗИ