

PALASINO

GROUP, A.S.

SOP #: ISO002-A

**SMĚRNICE: POLITIKA BEZPEČNOSTI INFORMACÍ**

Date Issued 23.11.2022  
 Revised: 15.08.2025  
 Authorization: Board of Directors  
 Next Review: 09.2026

**Verze dokumentu**

Verze	Autor	Změna	Popis změny
1.0		15.09.2022	Vytvoření dokumentu
1.1		23.11.2022	Revize dokumentu, doplněna legislativa v Příloze č.1
1.2	Kment	11.9.2023	Doplněn zákon č.171/2023 Sb.
1.3	Kment	24.10.2024	REVIZE DOKUMENTU
1.4	Kment	15.08.2025	Revize dokumentu, DLP

**Obsah**

<b>VYSVĚTLIVKY A DEFINICE .....</b>	<b>4</b>
<b>1. ÚČEL DOKUMENTU, KONTEXT ORGANIZACE A CÍLE INFORMAČNÍ BEZPEČNOSTI .....</b>	<b>6</b>
<b>2. POLITIKA BEZPEČNOSTI INFORMACÍ .....</b>	<b>7</b>
2.1. IDENTIFIKACE RELEVANTNÍCH ZÁKONŮ A NOREM.....	7
2.2. PŘEZKOUMÁNÍ POLITIKY BEZPEČNOSTI INFORMACÍ .....	8
<b>3. ŘÍZENÍ BEZPEČNOSTI INFORMACÍ .....</b>	<b>9</b>
3.1. KOORDINACE BEZPEČNOSTI INFORMACÍ .....	9
3.2. PŘÍRAZENÍ ODPOVĚDNOSTÍ V OBLASTI BEZPEČNOSTI INFORMACÍ .....	9
<i>Management PALASINO .....</i>	<i>9</i>
<i>Bezpečnostní forum (CARCOM).....</i>	<i>9</i>
<i>IT Security Manager .....</i>	<i>9</i>
<i>Liniový management.....</i>	<i>10</i>
<i>Pracovníci ICT .....</i>	<i>10</i>
<i>Vlastník aktiv.....</i>	<i>10</i>
<i>Uživatel - zaměstnanec .....</i>	<i>10</i>
<i>Externí – třetí strana .....</i>	<i>10</i>
<b>4. SPRÁVA AKTIV .....</b>	<b>11</b>
4.1. IDENTIFIKACE AKTIV .....	11
4.2. VLASTNICTVÍ AKTIV A RIZIK .....	11
4.3. INFORMAČNÍ AKTIVA .....	11
<b>5. POLITIKA MOBILNÍCH ZAŘÍZENÍ .....</b>	<b>13</b>

..... Z POHLEDU BEZPEČNOSTNÍCH OPATŘENÍ JE OBLAST POPSÁNA V UŽIVATELSKÉ PŘÍRUČCE BEZPEČNOSTI INFORMACÍ .....	14
<b>6. KLASIFIKACE INFORMACÍ .....</b>	<b>14</b>
<b>7. IDENTIFIKACE A KLASIFIKACE CITLIVÝCH DAT V RÁMCI SYSTÉMU DLP .....</b>	<b>16</b>
<b>8. BEZPEČNOST LIDSKÝCH ZDROJŮ .....</b>	<b>18</b>
8.1. PŘED UZAVŘENÍM PRACOVNÍ SMLOUVY .....	18
8.2. BĚHEM PRACOVNÍHO POMĚRU.....	18
<i>Program školení bezpečnosti informací .....</i>	<i>19</i>
<i>Disciplinární řízení .....</i>	<i>19</i>
8.3. UKONČENÍ NEBO ZMĚNA PRACOVNÍHO POMĚRU.....	20
<i>Ukončení poměru - odpovědnosti .....</i>	<i>20</i>
<i>Odstranění přístupových práv .....</i>	<i>20</i>
<i>Navrácení aktiv .....</i>	<i>21</i>
<b>9. FYZICKÁ A ENVIRONMENTÁLNÍ BEZPEČNOST .....</b>	<b>22</b>
9.1. CHRÁNĚNÉ OBLASTI .....	22
9.2. FYZICKÉ VSTUPNÍ KONTROLY .....	22
9.3. OCHRANA PŘED VNĚJŠÍMI HROZBAMI A PROSTŘEDÍ .....	23
<b>10. BEZPEČNOST KOMUNIKACÍ A PROVOZU .....</b>	<b>24</b>
10.1. PROVOZNÍ POSTUPY A ODPOVĚDNOSTI .....	24
10.2. MANAGEMENT ZMĚN .....	24
10.3. ODDĚLENÍ POVINNOSTÍ.....	24
10.4. ODDĚLENÍ VÝVOJE, TESTOVÁNÍ A PROVOZNÍCH ZAŘÍZENÍ.....	24
10.5. . OCHRANA PROTI ŠKODLIVÉMU KÓDU .....	25
<i>Kontrola proti škodlivému kódu .....</i>	<i>25</i>
10.6. ELEKTRONICKÉ ZASÍLÁNÍ ZPRÁV POUŽITÍM INTERNETU .....	25
10.7. ZÁLOHOVÁNÍ.....	25
10.8. MONITOROVÁNÍ .....	25
<b>11. ŘÍZENÍ PŘÍSTUPU .....</b>	<b>27</b>
11.1. POLITIKA ŘÍZENÍ PŘÍSTUPU.....	27
11.2. ŘÍZENÍ PŘÍSTUPU K SÍTI .....	27
11.3. ŘÍZENÍ PŘÍSTUPU K OPERAČNÍM SYSTÉMŮM .....	28
11.4. ŘÍZENÍ PŘÍSTUPU K APLIKACÍM.....	28
<b>12. ŘÍZENÍ FYZICKÉHO PŘÍSTUPU .....</b>	<b>29</b>
<b>13. AKVIZICE, VÝVOJ A ÚDRŽBA INFORMAČNÍCH SYSTÉMŮ .....</b>	<b>30</b>
13.1. POLITIKA BEZPEČNÉHO VÝVOJE.....	30
13.2. KRYPTOGRAFICKÉ KONTROLY .....	30
13.3. BEZPEČNOST PŘI TESTOVÁNÍ NOVÝCH FUNKCÍ IS .....	31
<b>14. PRAVIDLA VYUŽITÍ AI .....</b>	<b>32</b>
<b>15. MANAGEMENT BEZPEČNOSTNÍCH INCIDENTŮ.....</b>	<b>33</b>
15.1. HLÁŠENÍ BEZPEČNOSTNÍCH UDÁLOSTÍ A SLABIN.....	33
15.2. PŘÍKLADY BEZPEČNOSTNÍCH INCIDENTŮ .....	33
15.3. SPRÁVA BEZPEČNOSTNÍCH INCIDENTŮ A PROCES ZLEPŠOVÁNÍ .....	34
<i>Odpovědnosti a postupy.....</i>	<i>34</i>
<i>Ponaučení z bezpečnostních incidentů.....</i>	<i>34</i>
<i>Shromažďování evidence incidentů.....</i>	<i>34</i>
<b>16. MANAGEMENT KONTINUITY .....</b>	<b>35</b>
16.1. BEZPEČNOSTNÍ ASPEKTY ŘÍZENÍ KONTINUITY.....	35
16.2. TESTOVÁNÍ, ÚDRŽBA A PŘEZKOUMÁNÍ PLÁNŮ KONTINUITY.....	35

<b>17.</b>	<b>SHODA S BEZPEČNOSTNÍMI POŽADAVKY.....</b>	<b>36</b>
17.1.	OCHRANA DUŠEVNÍHO VLASTNICTVÍ.....	36
17.2.	OCHRANA DAT A OSOBNÍCH ÚDAJŮ.....	36
17.3.	DODRŽOVÁNÍ BEZPEČNOSTNÍCH POLITIK A STANDARDŮ, TECHNICKÁ SHODA.....	36
17.4.	HLEDISKA AUDITU INFORMAČNÍHO SYSTÉMU.....	37
	<i>Řízení auditu informačního systému.....</i>	<i>37</i>
	<i>Ochrana nástrojů auditu informačních systémů.....</i>	<i>37</i>
<b>18.</b>	<b>BEZPEČNOST INFORMACÍ PŘI PŘÍSTUPU EXTERNÍCH DODAVATELŮ A TŘETÍCH STRAN.....</b>	<b>38</b>
18.1.	IDENTIFIKACE AKTIV A PŘÍSTUPŮ.....	38
18.2.	DOKUMENTACE A ODSOUHLASENÍ POŽADAVKŮ S DODAVATELI.....	38
18.3.	PŘIŘAZENÍ ODPOVĚDNOSTÍ.....	38
18.4.	PRAVIDELNÉ KONTROLY A AUDIT.....	38
18.5.	UKONČENÍ PŘÍSTUPU A SPOLUPRÁCE.....	39
18.6.	VZOROVÉ BODY DO SMLOUVY/DOHODY.....	39

## Vysvětlivky a definice

V dokumentu jsou použity následující pojmy a zkratky:

<b>Termín</b>	<b>Definice</b>
Aktivum	cokoliv, co má hodnotu pro PALASINO.
BYOD	Bring You Own Device (přines si vlastní zařízení). Možnost používání osobních (soukromých) mobilních zařízení pro pracovní účely a jejich připojení k firemním datům PALASINO.
Dostupnost	vlastnost definující přístupnost a použitelnost aktiva tak, jak ji vyžaduje autorizovaný subjekt.
Důvěrnost	vlastnost, kdy informace není dostupná nebo prozrazena neoprávněným jedincům, subjektům nebo procesům.
Kontroly	způsoby řízení rizik, zahrnující politiky, postupy, směrnice, pracovní postupy nebo organizační struktury, které mohou být administrativní, technické, manažerské nebo právní podstaty. Kontroly jsou také použity jako synonymum pro zabezpečení nebo protipatření.
Nápravná opatření	opatření k vyloučení příčiny zjištěné neshody nebo jiné nežádoucí situace.
Událost	výskyt určitého souboru okolností.
Směrnice	doporučení očekávaných kroků, které mají vést k dosažení cíle.
ICT	Informační a komunikační technologie - zahrnují technologie a postupy, které se používají pro tvorbu, změny, distribuci, ukládání, mazání a obnovení dat a informací.
Dopad	nepříznivá změna ovlivňující úroveň dosažení obchodních cílů.
Bezpečnost informací	ochrana důvěrnosti, integrity a dostupnosti informací; tj. takové vlastnosti jako pravost, odpovědnost, nepopiratelnost, spolehlivost či důvěryhodnost.
Bezpečnostní událost	identifikovaný výskyt systému, servisu nebo stavu sítě označující možné porušení politiky bezpečnosti informací nebo selhání zabezpečení nebo předem neznámá situace, která může být relevantní k bezpečnosti.
Bezpečnostní incident	jednotlivé nebo série několika nechtěných či neočekávaných bezpečnostních událostí v bezpečnosti informací, které mají značnou pravděpodobnost pro kompromitaci business operací a ohrožení bezpečnosti informací.
Integrita	vlastnost zajištění správnosti a kompletnosti aktiv.
Intranet	je PALASINO síť (firemní síť) zahrnující všechny poskytované aplikace a informace.
Škodlivý software (malware)	je software, jehož aplikace/spuštění může způsobit uživatelem nekontrolovatelné,

	nebezpečné návaznosti – patří sem viry, červy, Trojské koně, mobilní kódy apod.
NDA (Non disclosure agreement)	dohoda o mlčenlivosti.
Politika	celkové záměry a směřování, jak je vyjadřuje management společnosti.
Preventivní opatření	akce k vyloučení příčiny možných neshod nebo jinak nežádoucích situací.
Procedura	specifický způsob k uskutečnění aktivity nebo procesu.
Proces	skupina mezi sebou příbuzných nebo navazujících aktivit, které mění vstupy ve výstupy.
Záznam	dokument bilancující dosažené výsledky nebo poskytující důkaz o proběhlých aktivitách.
Riziko	kombinace pravděpodobnosti události za určitých okolností.
Zbytkové riziko	riziko přetrvávající po ošetření rizika.
Akceptace rizika	rozhodnutí o akceptaci (zbytkového) rizika.
Analýza rizik	systematické použití informací k identifikaci zdrojů a k odhadu rizika.
Vyhodnocení rizika	celkový proces analýzy rizik a hodnocení rizik.
Rizikový management	koordinované aktivity k řízení a kontrole společnosti s ohledem k rizikům.
Ošetření rizik	proces výběru a implementace opatření k ovlivnění úrovně (snížení) rizik.
Zabezpečená oblast	je fyzická oblast se speciálními bezpečnostními kontrolami.
Standalone	izolovaný, nepropojený.
Hrozba	možná příčina nechtěného incidentu, která může vést k poškození ICT nebo společnosti.
Třetí strany	společnosti, které nejsou součástí PALASINO.
Uživatel	osoba, která má logický přístup k informačnímu systému a používá jeho služby a funkce.
VPN	Virtual Private Network označuje spojení místních sítí nebo jednotlivých PC např. prostřednictvím internetu. Je žádoucí použití vhodných pravidel chování takzvaných tunelů v rámci internetu. Data mohou být přenášena v rámci zúčastněných místních sítí a PC. Kryptografické kroky zajišťují důvěrnost a integritu přenášených informací v rámci tunelu. VPN může spojovat dva počítače (End-to-End-VPN), dvě sítě (Site-to-Site-VPN) nebo počítač a síť (End-to-Site-VPN).
Zranitelnost	Slabé stránky aktiv nebo řízení, které mohou být využity hrozbou.
CARCOM	Compliance and risk committee Bezpečnostní fórum
DLP	Technologie ochrany dat prostřednictvím technologie Microsoft Purview Information Protection (MIP) a Data Loss Prevention (DLP). Tato technologie umožnila nastavit a zavést jednotnou klasifikaci informací a odpovídající strukturu štítků citlivosti (MIP labels) dle interní analýzy potřeb.

## 1. Účel dokumentu, kontext organizace a cíle informační bezpečnosti

Účelem tohoto dokumentu Politiky bezpečnosti informací je vymezit základní strategie, cíle, principy, pravidla a související politiky týkající se bezpečnosti informací ve společnosti PALASINO GROUP, a.s. (dále jen "PALASINO"). Cílem je zajistit nezbytnou úroveň bezpečnosti informací a minimalizovat škody vzniklé vlivem bezpečnostních incidentů.

Informace jsou klíčovým podnikatelským aktivem a ochrana tohoto aktiva hraje zásadní roli při ochraně dlouhodobé ziskovosti firmy PALASINO. Kromě toho se prokazatelné silné řízení provozního rizika stává podstatným elementem pro vedení firmy a stále více i legislativním požadavkem. Vzhledem k tomu, že zabezpečení (nejen informací) je klíčovou oblastí provozního rizika, je rámec řízení bezpečnosti firmy primárním bezpečnostním mechanismem. Bezpečnost informací je jedním z prvků řízení bezpečnosti ve firmě.

Hlavní zásady budování bezpečnosti informací se týkají následujících oblastí:

Definice požadavků důvěrnosti, integrity a dostupnosti informací, které slouží k dosažení hospodářských a souvisejících cílů PALASINO.

Zajištění účinného předání požadavků osobám, které přicházejí do styku s takovými informacemi.

Zajištění nakládání (používání, správy a distribuce) s těmito informacemi v jakékoliv podobě (elektronické nebo fyzické) způsobem, který je v souladu s požadavky Politiky bezpečnosti informací.

Definování přijatelného použití aktiv PALASINO.

Prosazování řízení bezpečnosti založené na zjištěných rizicích s cílem maximalizovat návratnost investic do zabezpečení.

Každý zaměstnanec a externí pracovník PALASINO si musí být vědom nutnosti dodržování stanovených zásad při manipulaci s informacemi PALASINO v jakékoliv formě, kterých je vlastníkem nebo mu byly svěřeny.

Tyto zásady platí pro celé PALASINO.

## 2. Politika bezpečnosti informací

Hlavním cílem politiky bezpečnosti informací v PALASINO je vytváření, udržování a zlepšování komplexního a účinného systému řízení bezpečnosti informací a ochrany informací, zajištění dostatečné bezpečnosti vůči externím subjektům a odstranění přímých a nepřímých ztrát způsobených zneužitím, zničením, modifikací nebo nedostupností aktiv.

PALASINO deklaruje:

Dostupnost a integritu informací (informace nepoškozené, nepozměněné, úplné atd.) v čase a místě dle podnikatelských potřeb společnosti, pouze těm, kteří je potřebují pro svoji pracovní činnost, čímž je zachována důvěrnost informací dle stanovené klasifikace informací (veřejné, interní, chráněné).

Řízení celého životního cyklu informací, tzn. jejich zpracování od okamžiku získání nebo vytvoření až po jejich likvidaci.

Přijímání bezpečnostních opatření přímo úměrných aktuální míře rizik spojených s ohrožením bezpečnosti informací.

Pravidelným monitorováním, hodnocením rizik, řízením bezpečnostních incidentů, nápravnými a preventivními opatřeními budeme zvyšovat účinnost řízení bezpečnosti informací.

Politika bezpečnosti informací je závazná pro všechny zaměstnance PALASINO a zainteresované subjekty.

Zaměstnanci jsou soustavně vzděláváni a školeni v oblasti bezpečnosti informací.

Externí subjekty jsou smluvně zavázány k dodržování interních předpisů společnosti PALASINO s.r.o.

Porušení pravidel bezpečnosti informací je považováno za závažné porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci a je předmětem disciplinárního řízení.

Dodržování stanovených zásad při nakládání s informacemi, které vlastní nebo mu byly svěřeny v jakékoliv formě, všemi zaměstnanci PALASINO.

Každý zaměstnanec a externí pracovník má možnost ohlásit jakékoliv nesrovnalosti s touto politikou přímo svému vedoucímu nebo prostřednictvím emailu na adresu ISO@PALASINO.cz.

### 2.1. Identifikace relevantních zákonů a norem

Řada požadavků na bezpečnosti informací je založena na stávajících právních předpisech České republiky a jednotlivých států, kde PALASINO působí. Proto je nezbytné identifikovat relevantní zákony a právní předpisy týkající se bezpečnosti informací. Identifikace zákonných požadavků je v gesci Security Managera.

Seznam všech relevantních zákonů pro provoz PALASINO je v příloze č.1:

#### Přehled nejvýznamnějších zákonů pro PALASINO

Zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

Zákon č. 121/2000 Sb., o ochraně autorských práv, ve znění pozdějších předpisů.

Zákon č. 480/2004 Sb., o některých službách informační společnosti („Antispamový zákon“), ve znění pozdějších předpisů.

Zákoník práce - č. 262/2006 Sb.

Standard ČSN ISO/IEC 27001:2023.

Zákon č. 186/2016 Sb., o hazardních hrách ve znění pozdějších novel.

Vyhláška č. 208/2017 Sb., kterou se stanoví rozsah technických parametrů, jejichž prostřednictvím jsou provozovány hazardní hry, požadavků na ochranu a uchovávání herních a finančních dat a jejich technické parametry

Vyhláška č. 10/2019 Sb., o způsobu oznamování a zaslání informací a přenosu dat provozovatelem hazardních her, rozsahu přenášených dat a jiných technických parametrech přenosu dat

Zákon č. 89/2012 Sb., občanský zákoník

Související dokumenty

Tento dokument definuje systém řízení bezpečnosti informací ve společnosti PALASINO. Spolu se souvisejícími dokumenty upřesňuje zásady bezpečnosti informací v PALASINO a zaštiťuje ostatní dokumenty bezpečnosti informací určené pro uživatele (**Uživatelská příručka bezpečnosti informací PALASINO# ISMS 002**), pro administrátory ICT (**Administrátorská příručka bezpečnosti informací PALASINO# ISMS 003**) a pro Security Managera (**Pokyny pro Security managera PALASINO#ISMS 004**).

Všechny dokumenty ohledně bezpečnosti informací jsou přístupné v databázi firemní dokumentace.

## 2.2. Přezkoumání politiky bezpečnosti informací

Obsah, úplnost a aktuálnost stejně jako účinnost a efektivnost stávající verze politiky jsou pravidelně revidovány (minimálně jednou ročně) – toto je v kompetenci IT Security Managera.

Každá změna v organizaci bezpečnosti informací nebo v informačních aktivech, každý vážný bezpečnostní incident a nové významné zranitelnosti vedou k revizi a případně k aktualizaci této politiky.

Veškeré změny nebo rozšíření této směrnice musí být projednány s IT Security Managerem a schváleny vedením PALASINO.

## 3. Řízení bezpečnosti informací

### 3.1. Koordinace bezpečnosti informací

Vedení PALASINO ustanovilo roli IT Security Managera, jehož cílem je koordinovat aktivity v oblasti bezpečnosti informací. Má povinnost podporovat, rozvíjet a udržovat politiky bezpečnosti informací v praxi. IT Security Manager připravuje relevantní podklady pro jednání a rozhodování vedení PALASINO.

### 3.2. Přiřazení odpovědností v oblasti bezpečnosti informací

Odpovědnosti za zpracování informací a provoz informačního systému musí být jasně stanoveny a dokumentovány.

Management PALASINO

Vedení PALASINO deklaruje svou vůli a pozitivní přístup k řešení bezpečnosti informací. Realizace politiky bezpečnosti informací je zakotvena v odpovědnosti managementu, který má pro tento účel svěřené pravomoci. Vedení PALASINO vytváří podmínky pro tuto činnost a poskytuje zdroje potřebné pro realizaci obsahu a cílů politiky bezpečnosti informací.

Bezpečnostní forum (CARCOM)

Minimálně 2x ročně se schází bezpečnostní fórum PALASINO sestávající z příslušných lidí odpovědných za naplňování požadavků bezpečnosti informací.

Členy bezpečnostního fóra jsou: Director of Operation, Managing Director, Director HRA&F, Head of IT (ICT Manager ), IT Security Manager, Audit Manager, Compliance Manager, System Manager, Head of Marketing , Regionální finanční ředitel.

Odpovědnosti:

- Diskutuje klíčové iniciativy (nová rizika firmy) v oblasti bezpečnosti ICT a navrhuje řešení ke schválení vedením PALASINO.
- Koordinuje a reviduje činnosti v oblasti plnění stanovených cílů.
- Posuzuje relevantnost a přiměřenost politik v oblasti bezpečnosti informací a související dokumentace.
- Vytváří 1x ročně zprávu o bezpečnosti informací v PALASINO, která je založena na rizicích.
- Vytváří zápisy z jednání bezpečnostního fóra.
- Minimálně 1x ročně posílá zápisy z jednání bezpečnostního fóra a výroční zprávu bezpečnosti informací k rukám vedení PALASINO.

Nese konečnou odpovědnost za to, že je bezpečnost informací správně řízena.

IT Security Manager

Úkolem security manažera je řídit bezpečnost informací ve firmě PALASINO.

Odpovědnosti jsou podrobně popsány v bezpečnostní příručce **Pokyny pro IT Security Managera**.

### Liniový management

Je povinen zajistit, aby podřízení zaměstnanci byli dobře informováni a školeni. Dále je povinen zajistit spolupráci při řešení bezpečnosti informací v jejich rozsahu a podporu průběžného sledování bezpečnosti informací.

### Pracovníci ICT

Poskytují kompletní dokumentaci sítě, HW a evidenci SW licencí. Vykonávají správu v jejich gesci (sít, pracovní stanice, servery, zálohování, vedení uživatelských účtů, HW údržba, údržba operačního systému a antivirová ochranu). Správce aplikací stanovuje bezpečnostní mechanismy k ochraně informačních aktiv v souladu s přidělenou třídou klasifikace informací. Jsou zodpovědní za vynucení zabezpečení aplikací a a operačních systémů Další informace naleznete v **Administrátorské příručce bezpečnosti informací**.

### Vlastník aktiv

Vlastník aktiv je odpovědný za definici způsobu zpracování informací, jejichž je vlastníkem, a to tak, že definuje způsob ukládání informací, jejich klasifikaci a definuje bezpečnostní požadavky na ochranu svěřených aktiv.

### Uživatel - zaměstnanec

Všichni zaměstnanci jsou v rámci svých kompetencí odpovědní za dodržování předpisů pro bezpečnosti informací. Detailní informace naleznete v **Uživatelské příručce bezpečnosti informací**.

### Externí – třetí strana

V případě přístupu třetí strany k informacím nebo informačním systémům společnosti, osoba, která zaměstnává nebo řídí vztah se třetí stranou, musí zajistit, že zaměstnanci této třetí strany jsou informováni, poučeni, proškoleni a zavázáni dodržováním bezpečnostních předpisů PALASINO.

Pro každý přístup externí firmy k IS PALASINO musí existovat platný kontrakt. Při sjednávání služeb externí firmy musí být posouzena a stanovena míra rizika spojená s přístupem třetí strany do IS PALASINO.

Všechny požadavky bezpečnosti informací musí být součástí smluvních ujednání (příp. NDA) se třetími stranami. Smlouvy musí být schváleny a oboustranně podepsány dříve, než třetí strana obdrží přístup k aktivům PALASINO. Přístup externistů musí být striktně omezen na nezbytně nutný rozsah, který je potřebný pro plnění sjednaných služeb a závazků. Přístup externistů může být monitorován zejména tehdy, pokud třetí strana používá další subdodavatele. Tyto smlouvy (zejména pak vzor NDA) musí být pravidelně přezkoumávány, což je v kompetenci IT Security Managera.

## 4. Správa aktiv

### 4.1. Identifikace aktiv

Všechna relevantní aktiva musí být identifikována. Aktiva (SW, HW, služby, data, informace atd.) mají pro organizaci PALASINO hodnotu, a proto vyžadují odpovídající ochranu.

#### Klasifikace aktiv:

- fyzická aktiva;
- aplikační a programová aktiva;
- informační a datová aktiva;
- lidské zdroje, know-how;
- služby.

### 4.2. Vlastnictví aktiv a rizik

Pro každé z těchto aktiv je v seznamu aktiv definován vlastník (definovaný vlastník je osoba, která je zodpovědná za konkrétní organizační jednotku PALASINO). Vlastník je odpovědný za:

- stanovení úrovně potřebné ochrany a odpovídající ochranné mechanismy, včetně přístupových práv (fyzický a logický přístup);
- ohodnocení rizik aktiva;
- určení vlastníka rizika, který je odpovědný za realizaci ochranných mechanismů;
- platnost realizovaných ochranných mechanismů i v době, kdy je aktivní práce s aktivem již ukončena (např. informace mají nadále nastavena adekvátní přístupová práva i v archivu, mimo aktivní systém).

### 4.3. Informační aktiva

Každé informační aktivum je posuzováno a hodnoceno z hlediska důležitosti a citlivosti. Cílem tohoto hodnocení je stanovení priorit nezbytných pro definici požadavků na ochranu a obnovu aktiv v případě nouze.

Definice a hodnocení informačních aktiv je výchozím krokem pro analýzu rizik. Vyhodnocení a stanovení priorit obnovy je definováno vlastníkem informačního aktiva.

Odpovědnost za informační aktiva je rozdělena do několika oblastí:

- IT Security Manager navrhuje přidělení aktiva a na základě schválení CARCOM a BOD přiděluje aktiva jejich příslušným vlastníkům.
- Identifikace, klasifikace a hodnocení informačních aktiv jsou v působnosti jejich vlastníka (vlastník aktiva může přenést odpovědnost na svého zástupce a ustanovit jej vlastníkem rizika spojeného s aktivem).
- Bezpečnostní fórum stanovuje bezpečnostní mechanismy na ochranu informačních aktiv adekvátně přidělené klasifikaci informací.
- Vlastník rizika je odpovědný za realizaci bezpečnostních ochranných mechanismů.

U každého informačního aktiva IS je definován vlastník, který je odpovědný za jeho řízení.

Vlastníkem aktiv nebo definované skupiny informačních aktiv v rámci ICT oddělení je obvykle vedoucí zaměstnanec, v rámci jehož odpovědnosti je správa aktiva v rámci IS. Tj. vlastníkem aktiva, o které se stará např. programátor je Manager ICT – ten však může vlastnictví aktiva delegovat na Systémového technika apod. Systémový technik je pak ustanoven vlastníkem rizika např. ztráty dat a provádí bezpečnostní ochranný mechanismus, který spočívá v zálohování dat.

Vlastník informačních aktiv je zodpovědný za:

Posouzení a stanovení hodnot a priorit informačních aktiv nebo klasifikaci informačních aktiv v rámci vlastní pravomoci.

Stanovení požadavků na ochranu aktiv IS (lhůty pro zajištění kontinuity, požadavky na zálohování atd.).

Management informačních aktiv IS (pravidla pro údržbu a kontrolu, přesnost a úplnost, označování, výměny aktiv) v souladu s definovanými pravidly.

Výmaz dat je prováděn v souladu s relevantní legislativou (např. ZHH 2 roky pro kamerové záznamy), data ve fyzické podobě jsou likvidována dle Spisového a skartačního řádu OPS 65. Maskování dat se využívá například pro následující situace: Hráčský ID (HID) nebo maskování v reportech MF.

## 5. Politika mobilních zařízení

Politika používání mobilních zařízení je platná pro firemní zařízení i pro soukromá zařízení (BYOD). Z pohledu evidence majetku, správy a zabezpečení včetně přidělování je celá oblast detailně popsána v následujících interních směrnicích: SOP#: ADM 26, SOP#: ADM 37,

- postup při přidělování mobilních zařízení
- správu a dokumentaci o přidělených mobilních zařízeních a sim kartách
- zabezpečení mobilních firemních zařízení a ochrana osobních údajů
- ztráta, krádež zařízení, zablokování zařízení, převod sim
- typ, hodnoty zařízení dle jednotlivých pozic ve společnosti
- limity pro maximální vyúčtování zvláštní pokyny

## 6. Z pohledu bezpečnostních opatření je oblast popsána v Uživatelské příručce bezpečnosti informací. Klasifikace informací

U všech aktiv provede příslušný vlastník ohodnocení jejich důvěrnosti, integrity a dostupnosti. Výsledná hodnota je podkladem Analýzy rizik, která stanovuje adekvátní způsob ochrany aktiv dle výsledných rizik.

Pro zavedení klasifikace pro všechna média obsahující informace (např. databáze, servery, paměťová média, v sítích, na papíře, přenos mluveného slova), je zapotřebí tyto způsoby nakládání s informacemi také třeba vzít v úvahu pro stanovení pravidel pro klasifikaci informací.

V rámci PALASINO jsou k označování odpovídajícího stupně klasifikace informací používány informační štítky (popisky, metadata). Označování je povinné pro každého autora informací.

V rámci ochrany dat byla zavedena technologie ochrany dat prostřednictvím technologie Microsoft Purview Information Protection (MIP) a Data Loss Prevention (DLP). Tato technologie umožnila nastavit a zavést jednotnou klasifikaci informací a odpovídající strukturu štítků citlivosti (MIP labels), které umožnili úměrně klasifikovat a chránit dokumenty podle úrovně citlivosti a důvěrnosti. Zavedením DLP zásad je automatizovaně zajišťována prevence neautorizovaných přenosů nebo sdílení citlivých informací napříč organizací i při externí komunikaci. Dále nám tato technologie umožnila tajstit centralizované monitorování, auditování a reporting incidentů souvisejících s únikem nebo nedovolenou manipulací s citlivými daty.

Kategorizace všech informací je založena na níže stanovené základní klasifikační stupnici. Tato stupnice je dále rozšířena pro štítky v rámci ochrany dokumentů DLP.

### Veřejné údaje

Termínem „veřejné údaje“ jsou označována data, která mohou být zveřejněna, aniž by jejich uveřejnění mělo na organizaci negativní dopad. Tato data mohou být veřejně vynášena (elektronicky i v papírové podobě) z prostředí organizace, šířena po internetu, elektronickou poštou apod.

Veřejné údaje nepodléhají požadavkům na ochranu před nepovolaným přístupem. Tím však nejsou dotčeny požadavky na ochranu těchto dat před poškozením, zničením či úmyslnou změnou, což by ovlivnilo jejich integritu, případně mělo za následek jejich nedostupnost. Veřejné údaje tak logicky tvoří první, i když z hlediska ochrany nejnížší stupeň klasifikace dat organizace.

Informace mohou být přijímány odkudkoliv.

Informace mohou být předány komukoliv.

Není požadována žádná ochrana informace.

Veřejné údaje: data zveřejněná na webových stránkách PALASINO, marketingové prezentace společnosti, reklamní materiály a nevyplněné formuláře (klienti, uchazeči o zaměstnání apod.)

### **Bez označení - veřejné informace jsou pouze výše výčtem uvedené**

### Interní údaje

Další kategorií identifikovaných dat zpracovávaných v IS PALASINO jsou údaje, které jsou přístupné všem zaměstnancům organizace, ale nejedná se o veřejné údaje.

Informace smějí získat pouze zaměstnanci PALASINO.

Informace mohou být předány pouze zaměstnancům PALASINO.

Je požadována ochrana proti externímu přístupu k informacím.

Příklady: vnitřní předpisy, interní katalog, ceníky, pracovní postupy, poptávky

**Tyto údaje jsou bez označení**

### **Chráněné údaje**

Chráněné údaje představují kategorii identifikovaných dat zpracovávaných v IS PALASINO, které mohou být snadno zneužity ku prospěchu (finančnímu, hmotnému aj.) osobou, která k nim může přistupovat oprávněně i neoprávněně (zevnitř organizace i zvenčí). Tyto údaje nejsou veřejné. Jsou určeny pouze vybraným skupinám uživatelů a podléhají ochraně před neoprávněným přístupem.

Jedná se například o:

- osobní údaje,
- údaje obchodního tajemství,
- údaje chráněné zákonem o kybernetické bezpečnosti v platném znění,
- důvěrné a utajované informace vázané smluvním zajištěním při práci u zákazníků,
- mzdové údaje;
- finanční údaje;
- apod.

Chráněné informace jsou uvnitř organizace distribuovány prostřednictvím intranetu a elektronické pošty s omezeným přístupem uživatelů.

V případě existence chráněných informací ve fyzické podobě se musí označit prostory "Sensitivity level –C".



Dokumenty v elektronické formě jsou označovány jejich vlastníkem a dále prostředky informačního systému M365.

**S jakýmkoli neoznačenými informacemi PALASINO musí být vždy zacházeno jako s interními.**

Technické vlastnosti podnikových systémů, např. funkce e-mailových systémů (např. šifrování, prevence přesměrování, označování) jsou používány pro podporu implementace odpovídajících opatření vyplývajících z konkrétní úrovně klasifikace informací.

## 7. Identifikace a klasifikace citlivých dat v rámci systému DLP

Na základě analýzy a stanovené kategorizace typů citlivých informací dle interních a regulatorních požadavků s využitím funkcionalit Microsoft Purview pro automatickou identifikaci citlivých dat (Sensitive Information Types) byla definována klasifikační stupnice a implementována odpovídající sada štítků (labels) citlivosti, které umožňují přesně klasifikovat data dle úrovně důvěrnosti:

Klasifikace *Public*

7.1. Odpovídající štítek citlivosti *Public*

Klasifikace *Internal*

7.2. Odpovídající štítek citlivosti *Internal*

Klasifikace *Confidential*

7.3. Odpovídající štítky citlivosti dle účelu použití:

7.3.1. *Confidential / General Use*

7.3.2. *Confidential / Finance*

7.3.3. *Confidential / Compliance*

7.3.4. *Confidential / HR*

7.3.5. *Confidential / External (no protection)*

Klasifikace *Highly Confidential*

7.4. Odpovídající štítky citlivosti dle účelu použití:

7.4.1. *Highly Confidential / User Defined*

7.4.2. *Highly Confidential / BOD*

Změny nastavení oprávnění uživatelů u štítků aplikujících na obsah ochranu šifrováním stejně jako změny v členství ve skupinách uživatelů, kterým jsou štítky publikovány, probíhají v rámci řízených interních procesů organizace.

Aplikace klasifikačních štítků probíhá primárně ručně uživateli.

Každý nový nativně podporovaný dokument (Office, PDF) má automaticky přiřazen štítek *Internal*. Je na zvážení uživatele, zda automaticky přiřazený štítek odpovídá skutečné klasifikaci dokumentu nebo je potřeba klasifikaci snížit nebo zvýšit.

Aplikace štítků je vynucována pro dokumenty. Tzn. dokument nelze uložit bez aplikovaného štítku.

Aplikace štítků není vynucována pro emaily.

Případné snížení klasifikace dokumentu vyžaduje od uživatele zdůvodnění, které je následně součástí auditního logu o operaci.

### Opatření k nakládání s chráněnými informacemi

- Pro diskusi o chráněných informacích zvolit takové prostory, kde je obtížné rozhovor odposlouchávat.
- Chráněné informace nenechávat jako odkaz v hlasové schránce.
- Při předávání chráněných informací (nezávisle na způsobu) je povinností toho, kdo informaci předává, ověřit identitu příjemce informace a jeho oprávnění k této informaci, a zajistit, aby k informaci neměli přístup neoprávněné osoby.
- Dávat si pozor na techniky sociálního inženýrství a neposkytovat chráněné informace osobám, o jejichž identitě, oprávnění pro přístup k informacím nebo důvodu žádosti o informace existují jakékoliv pochybnosti.

- chráněné informace třetích stran chránit stejným způsobem jako chráněné informace PALASINO.
- Přístup třetích stran k chráněným informacím společnosti je možný jen po uzavření dohody o mlčenlivosti (NDA), respektive po nastavení technických / organizačních pravidel na ochranu těchto informací.
- Přenášení chráněných informací na počítače mimo řízení společnosti za účelem jejich dalšího zpracování (typicky dokončení práce na domácím / soukromém počítači přes víkend apod.) pomocí USB médií, soukromé emailové schránky, resp. Jiným způsobem není povoleno – informace společnosti lze zpracovávat pouze na zařízeních ve správě společnosti.
- Ztrátu nebo krádež dokumentů, datových médií, mobilních telefonů a notebooků obsahující chráněná data je pracovník povinen neprodleně hlásit nadřízenému pracovníkovi.

## 8. Bezpečnost lidských zdrojů

Pravidla a pracovní podmínky (např. pracovní smlouvy, pracovní předpisy, pracovní instrukce) definují odpovědnost jednotlivých zaměstnanců za bezpečnost informací.

Jsou specifikovány a realizovány fáze pokrývající období celého pracovního poměru (před / během / změna / ukončení).

### 8.1. Před uzavřením pracovní smlouvy

Informace týkající se potenciálního zaměstnance jsou shromažďovány a ověřovány definovaným standardizovaným HR procesem.

Všichni budoucí zaměstnanci budou v rámci přijímacího řízení prověřeni personalisty. Ověřeny budou:

- reference z předchozích zaměstnání a případné osobní hodnocení dle potřeby,
- písemné doklady o získané kvalifikaci, je-li pro danou pracovní pozici požadována,
- výpis z rejstříku trestů.

Příslušná povinná školení pro nové zaměstnance jsou definována, prováděna a záznamy jsou shromažďovány.

Každý nový zaměstnanec je seznámen s PALASINO pravidly (např. interní předpisy, Uživatelská příručka bezpečnosti informací) a podepisuje dokument o seznámení s interními předpisy a pravidly zacházení s informacemi a doklady.

Ustanovení týkající se mlčenlivosti a autorských práv musí být součástí všech smluv o obchodním zastoupení a smluv se zaměstnanci třetích stran.

Je nutné vyplnit „Žádost o přidělení přístupové karty“ a případně i založení nového uživatele systémů. Pro případ vydání zaručeného elektronického podpisu zaměstnanci, který má právo jednat za firmu vůči orgánům státní správy v předem definovaných oblastech je nutné provést veškeré úkony a kroky v souladu s interní procedurou *ADM 38 IT - Vydávání zaručených a nezaručených elektronických podpisů*.

### 8.2. Během pracovního poměru

Každý zaměstnanec PALASINO si musí být zcela vědom a je povinen:

- dodržovat stanovené zásady při manipulaci s informacemi, které vlastní nebo mu byly svěřeny ze strany PALASINO, a to v jakékoliv podobě;
- dodržovat interní předpisy a nařízení ohledně nakládání s informacemi a dokumenty;
- být v souladu s vnitřními předpisy.

Výše uvedený závazek v souladu se současnými politikami je závazný pro všechny zaměstnance PALASINO.

Nedodržení Politiky bezpečnosti informací a související dokumentace může vést k disciplinárnímu řízení.

#### Program školení bezpečnosti informací

Předtím, než uživatel získá přístup k informacím a / nebo informačním a komunikačním systémům, je povinen jeho přímý nadřízený (vedoucí oddělení) zajistit vhodné školení, pokyny, vysvětlení, informace, aby:

- uživatel si byl vědom bezpečnostních hrozeb a rizik, jakož i mechanismů pro prevenci možných bezpečnostních chyb a znal svou vlastní zodpovědnost v této souvislosti;
- uživatel byl schopen odborně zpracovávat informace a používat systémy v souladu se všemi platnými předpisy.

Školení o bezpečnosti informací má za úkol vzdělávání zaměstnanců v těchto oblastech:

- vhodné použití, ochrana a bezpečnost informací;
- individuální odpovědnost a průběžné činnosti nutné k ochraně důvěrnosti, integrity a dostupnosti informačních aktiv, zdrojů a systémů proti neautorizovanému přístupu, použití, zneužití, zveřejnění, zničení, změna nebo zničení;
- správné využívání informačních aktiv, zdrojů a systémů (logické postupy, politika hesel, politika internetu, e-mailová politika, šifrování, škodlivý software a nelegální software);
- znalost bezpečnostních hrozeb a způsobu nakládání s informacemi;
- organizace bezpečnosti informací;
- pochopení politiky bezpečnosti informací, plnění kontrol, vnitřních auditů a nápravných opatření.

Materiál o školení bezpečnosti informací je k dispozici na intranetu PALASINO a u IT Security Managera. Odkaz: <https://twhe.sharepoint.com/ppm/TWHE%20SOPs/Forms/AllItems.aspx>

Školení bezpečnosti informací musí povinně absolvovat každý zaměstnanec PALASINO nebo dodavatel s přiděleným přístupem k PALASINO aktivům – informacím nebo informačním systémům (NEON apod.).

O veškeré změny v procedurách a informace o nově vydaných procedurách je zasíláno všem, kteří mají přístup k emailovému účtu prostřednictvím RSS odkazu a emailového odkazu. Pro zaměstnance bez přístupu k emailovému účtu jsou informace o změnách vyvěšovány na zaměstnaneckých nástěnkách nebo prostřednictvím interních facebook upozornění. Pokud dojde k významné změně a doplnění, je procedura znovu proškolená přes systém Edunio.

#### Disciplinární řízení

Ačkoli lze obecně předpokládat, že všichni zaměstnanci PALASINO jsou na dostatečné morální úrovni, mají odpovídající školení o bezpečnosti informací a jsou si vědomi své spoluodpovědnosti za ochranu informací a aktiv, jsou pro účely disciplinárního řízení, zejména jako preventivní opatření, stanoveny sankce.

Zneužití počítačových, e-mailových systémů nebo počítačové sítě poskytnutých společností v rozporu se zákonem nebo firemními postupy povede k disciplinárnímu řízení, včetně rozvázání pracovního poměru a následnými právními kroky na ochranu společnosti a zaměstnanců.

Zaměstnanci mohou zároveň nést osobní odpovědnost za jakékoliv porušení tohoto postupu.

Sankcemi se trestá nedbalost nebo úmyslné porušení bezpečnostních předpisů.

Sankce jsou uplatňovány v souladu s právní úpravou v případě porušení povinností vyplývajících z právních předpisů vztahujících se k vykonávané práci, včetně předpisů bezpečnosti informací, ze strany uživatele na základě posouzení závažnosti a míry zavinění určitého rizika nebo rozsahu dopadu a důsledků bezpečnostních incidentů způsobených porušením politiky bezpečnosti informací.

Tyto sankce mohou být například:

- změna nebo zrušení přístupových práv do informačního systému, popř. k informacím jako aktivu obecně;
- výpověď ze strany zaměstnavatele;
- právní sankce;
- trestní oznámení.

PALASINO si vyhrazuje právo kontrolovat a monitorovat dodržování firemních předpisů a vhodně reagovat na narušení bezpečnostní politiky a zneužívání s ohledem na příslušné právní a obchodní zákony v současné platnosti. Za tímto účelem může být na pokyn vedení společnosti, příp. bezpečnostního fóra kontrolována i emailová komunikace zaměstnanců zasílaná prostřednictvím firemní emailové schránky v souladu s § 316 Zákonníku práce.

Toto právo zaměstnavatele je popsáno v pracovních předpisech, pracovních smlouvách a jiných podobných dohodách. Navíc může porušení právních předpisů, ve vztahu k bezpečnosti informací, také vést k trestnímu stíhání.

Jedná se zejména o tyto trestné činy dle Trestního zákoníku (zákon č. 40/2009 Sb.)

- § 230 - Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 - Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

### 8.3. Ukončení nebo změna pracovního poměru

Ukončení poměru - odpovědnosti

Pro ukončení pracovního poměru je vystaven EXIT FORM a jsou informováni zodpovědní zaměstnanci pro doplnění údajů o ukončení přístupů a vrácení aktiv společnosti. Vedoucí zaměstnanec informuje ICT oddělení bez prodlení, pokud jde o jakékoliv skončení pracovního poměru nebo změnu pozice zaměstnance (zrušení uživatele).

Odstranění přístupových práv

Žádost o zrušení přístupových práv a přístupové karty musí být vyplněna pro realizaci v rámci vystaveného EXIT FORM personálním oddělením. O existenci EXIT FORM je ICT oddělení informováno odkazem v HelpDesk zasláním založení Exit Form se jménem a osobním číslem zaměstnance na email [exitform@helpdeskmail.PALASINO.cz](mailto:exitform@helpdeskmail.PALASINO.cz). ICT oddělení odebere všechna přístupová práva odcházejícího zaměstnance a zapíše realizaci do EXIT FORM. Proces ukončení pracovního poměru či přerušení výkonu práce z důvodu například nástupu na mateřskou či rodičovskou dovolenou nebo při dlouhodobějším přerušení pracovního výkonu vede k odebrání přístupových práv, případně k přesměrování emailové pošty na určitou dobu.

Žádost o zrušení přístupových práv a přístupové karty musí být vyplněna pro realizaci v rámci vystaveného formuláře EXIT FORM personálním oddělením. O existenci EXIT FORM je ICT oddělení informováno automaticky odkazem v ICT HelpDesku poté co je soubor personálním oddělením ve formátu názvu souboru "Exit Card JmenoPrijmeni OSCislo" nahrán na SharePoint nebo do lokálně synchronizované SharePoint složky. ICT oddělení následně odebere všechna přístupová práva odcházejícího zaměstnance a zapíše realizaci do EXIT FORM. Proces ukončení pracovního poměru či přerušení výkonu práce z důvodu například nástupu na mateřskou či rodičovskou dovolenou nebo při dlouhodobějším přerušení pracovního výkonu vede k odebrání přístupových práv, případně k přesměrování emailové pošty na určitou dobu.

### Navrácení aktiv

Odcházející zaměstnanci jsou povinni vrátit veškerá aktiva (např. HW – počítače, mobilní telefon, přístupové karty, kreditní karty, klíče, Fido klíče, tokeny atd.), která získali (dle seznamu) v průběhu své činnosti na příslušné oddělení, ze kterého je obdrželi. Toto je součást EXIT FORM.

## 9. Fyzická a environmentální bezpečnost

### 9.1. Chráněné oblasti

Informace a systémy se zvýšenými bezpečnostními požadavky musí být umístěny v oddělených prostředích, která jsou označována jako "chráněné oblasti" na základě stanovené klasifikace aktiv.

Jednotlivá oddělení (HR oblast, finanční, ICT, atd.) využívají uzamčené skříně a uzamčené kanceláře pro ukládání zabezpečených informací v režimu „**Sensitivity level - C**“. ICT oddělení dále používají prostředky pro produkční a testovací prostředí tj. pro servery v serverové místnosti, pro ICT infrastrukturu - serverovna, rackové skříně, úložné prostory pro hardware a software.



Chráněné oblasti jsou rozděleny do následujících kategorií:

- prostory veřejně přístupné;

- interní prostory za vstupními dveřmi, recepcemi;

- prostory s dodatečným zabezpečením nad rámec interních prostor (serverovny, rozvodny energií).

### 9.2. Fyzické vstupní kontroly

Přidělení fyzických přístupových práv k chráněné oblasti je regulováno a dokumentováno.

Definované fyzické vstupní kontroly (např. klíčový režim budov, místností, skříní pro klasifikovaná data) musí být dokumentovány.

Fyzický přístup k zabezpečené oblasti je omezen pouze na oprávněné osoby s ohledem na potřebu nouzového vstupu (např. složky IZS).

Ověřovací média (klíče, přístupové kódy EZS) jsou zdokumentována a pravidelně přezkoumávána.

Zvláštní pravidla pro návštěvníky jsou implementována pomocí těchto kontrol:

- doprovod odpovědného zaměstnance PALASINO nebo vázaného externího pracovníka;

- omezení možnosti pohybu je dáno perimetrem chráněné oblasti.

- Hráči – viz pokyny v rámci Herního plánu a Návštěvního řádu provozoven.

### 9.3. Ochrana před vnějšími hrozbami a prostředí

Je k dispozici systém EZS, který musí být vhodně umístěn a pravidelně kontrolován.

Je realizováno UPS zálohování a NZ-dieselagregát pro servery, které je dokumentováno a pravidelně kontrolováno.

Záložní média s daty PALASINO jsou ukládána na bezpečné místo dle definovaného scénáře.

Klimatizace musí být pravidelně servisována.

Další informace v PALASINO # 002 ISMS **Administrátorské příručce bezpečnosti informací.**

## 10. Bezpečnost komunikací a provozu

### 10.1. Provozní postupy a odpovědnosti

Všechny hlavní provozní procesy, které jsou zajišťovány pomocí informačních a komunikačních technologií, musí být identifikovány, dokumentovány a řízeny tak, aby byla zajištěna jak bezpečnost, tak kontinuita těchto procesů.

### 10.2. Management změn

Provádění změn musí být kontrolováno pomocí formálních postupů řízení změn a je realizováno systémem Helpdesk a PALASINO SharePoint na dokumentačním serveru.

Postupy pro kontrolu změn jsou zdokumentovány a prosazovány s cílem minimalizovat poškození informačních systémů. Zavádění nových systémů a významných změn do stávajících systémů podléhá formálnímu procesu dokumentace, specifikace, testování, řízení kvality a řízené implementace schválených změn.

### 10.3. Oddělení povinností

Rozdělení povinností je metoda pro snížení rizika náhodného nebo úmyslného zneužití systému. Je třeba dbát na to, že žádný člověk nemůže měnit, používat nebo mít přístup k aktivům bez povolení nebo pověření.

Povinnosti a oblasti působnosti jsou odděleny, aby se snížily příležitosti k neoprávněné nebo neúmyslné změně nebo zneužití aktiv organizace.

K tomuto účelu je využíváno sledování aktivit, auditů a dohled nad řízením.

Bezpečnostní audit zůstává nezávislý – oddělený od procesů správy aktiv.

Oddělení povinností je popsáno v PALASINO # 002 ISMS **Administrátorské příručce bezpečnosti informací**.

### 10.4. Oddělení vývoje, testování a provozních zařízení

Vývoj, testování a provoz ICT zařízení je oddělen tak, aby se snížilo riziko neoprávněného přístupu nebo změny operačního systému, riziko náhodné změny nebo neoprávněného přístupu k datům PALASINO.

Měly by být určeny jednotlivé úrovně oddělení rolí na operační, testovací a vývojové, což je nezbytné k zabránění provozních problémů, a měly by být prováděny vhodné kontroly.

Servery pro vývoj jsou fyzicky odděleny od provozu.

## 10.5. . Ochrana proti škodlivému kódu

Kontrola proti škodlivému kódu

S cílem zajistit odpovídající ochranu proti malware (např. viry) v rámci společnosti jsou definována a implementována následující opatření:

Systemy ICT nejsou v defaultní konfiguraci.

Odpovídající anti-malware SW je instalován a pravidelně aktualizován na emailových serverech, pracovních stanic a vstupní bráně do sítě PALASINO.

Musí být instalovány relevantní záplaty pro operační systémy a veškerý software nainstalovaný na všech pracovních stanicích, serverech a dalších systémech.

Musí být prováděno pravidelné testování proti výskytu malware včetně evidence.

Nedodržení opatření vede ke vzniku bezpečnostního incidentu a k nápravným opatřením.

Všichni uživatelé a správci ICT PALASINO postupují podle pokynů popsanych v **Uživatelské příručce bezpečnosti informací** nebo **Administrátorské příručce bezpečnosti informací**.

## 10.6. Elektronické zasílání zpráv použitím internetu

Pro pracovní účely musí být použity pouze e-mailové systémy a datová schránka PALASINO, poskytované společností PALASINO. Pro soukromé účely není e-mailový systém zaměstnancům PALASINO poskytován.

Musí být dodržována nařízení týkající se šíření informací, včetně použití vhodných technik šifrování klasifikovaných informací (chráněné) případně použití zasílání prostřednictvím zabezpečených úložišť v rámci systému PALASINO.

Více informací v PALASINO # 001 ISMS **Uživatelské příručce bezpečnosti informací** nebo PALASINO # 002 ISMS **Administrátorské příručce bezpečnosti informací**.

## 10.7. Zálohování

Aby byla zaručena dostupnost informací a ICT systémů, je proces zálohování řešen na dvojí úrovni – uživatel a správce ICT.

Uživatel je zodpovědný za zálohování nestandardních aplikací a programů lokálně instalovaných na jeho pracovišti a informací v rámci jeho individuálního uživatelského prostředí. Uživatelé jsou seznámeni s politikou zálohování prostřednictvím dokumentu – PALASINO # 001 ISMS **Uživatelská příručka bezpečnosti informací**.

Zálohovací předpisy jsou plně definovány v PALASINO # 002 ISMS **Administrátorské příručce bezpečnosti informací**.

## 10.8. Monitorování

Systemy a aplikace se musí v souladu s platnými předpisy (např. zákony, směrnicemi) monitorovat dle Plánu monitoringu a kontrol

Neúspěšné pokusy o přihlášení do všech systémů a k informacím musí být zaznamenávány. Je-li to vyžadováno, konkrétní vlastník aktiva může požádat o záznamy možných typů selhání v rámci systémů v jeho gesci. Logy se záznamy selhání či zneužití musí být pravidelně vyhodnocovány kvalifikovanou osobou.

Relevantní záznamy selhání či zneužití musí systém zaznamenávat automaticky (hardware, software), nebo pomocí uživatelů, a musí platit:

Záznamy musí být analyzovány.

Dle konkrétního typu záznamu je zaměstnanec povinen provést nápravná opatření.

Dle konkrétního typu záznamu je zaměstnanec povinen provést preventivní opatření po zvládnutí akce nápravných opatření.

Všechny komponenty systému, které jsou předmětem monitoringu, musí mít synchronizovaný čas s ohledem na časové zóny a letní čas.

Více informací v PALASINO # 002 ISMS **Administrátorské příručce bezpečnosti informací**.

## 11. Řízení přístupu

### 11.1. Politika řízení přístupu

Registrace a veškeré následné změny nebo zrušení uživatele nebo skupiny přístupů jsou předmětem příslušných procesních předpisů. Takové procesy jsou striktně založeny na Žádosti o zřízení přístupu. Požadavek podléhá schválení příslušným vlastníkem dat a přímým nadřízeným uživatele. Veškerá evidence udělování přístupů do jakéhokoliv firemního systému nebo změna musí být evidovaný v IT Helpdesku v sekci "NEON CMS + Access" pro žádosti týkající se systému NEON a sekci "Uživatelské účty" pro další systémy (přístup do počítače, docházka apod.) Všechny požadavky pro resetování hesla nebo jiných problémů týkající se přístupu musí být vyžádány pomocí PALASINO IT Helpdesk systému. Změny, které nebudou evidované přes IT Helpdesk nejsou povoleny.

HR/personalista nebo nadřízený zaměstnanec musí informovat IT oddělení o každé změně pozice, která může ovlivnit přístup zaměstnanců do počítačové sítě Společnosti. Toto se týká především ukončení pracovního poměru a vystavení EXIT FORM, či dlouhodobou nepřítomnost, například mateřská dovolená. Všechny změny musí být evidovány přes IT Helpdesk.

Odebrání přístupových práv se provádí ihned po založení EXIT FORM a k datu odchodu zaměstnance.

Je zajištěno, že aplikace a informace jsou chráněny proti neoprávněnému použití a nežádoucím přístupům.

Bezpečnost a praktické uplatňování postupů jsou přezkoumávány v pravidelných intervalech, aby byly v souladu s technickými a organizačními změnami.

Pravidelná kontrola již přidělených přístupů:

Jednou za šest měsíců, IT administrátor vygeneruje přehled zaměstnanců a jejich přístupových práv pro kritických počítačové systémy a předá je k ověření vedoucím příslušných oddělení.

*Management of user accounts for access to company resources IT Správa Uživatelských účtů (ADM 21-02)*

Tyto údaje musí být ověřeny a schváleny vedoucím oddělení do dvou týdnů od obdržení. Email potvrzující výsledek kontroly, příp. správnost dat archivuje IT administrátor jako přílohu tasku v IT helpdesku, aby byl dostupný pro případnou kontrolu Audit oddělením.

Tyto systémy zahrnují NEON, SAP, Datové schránky, ELO, BYZNYS .

Více informací viz PALASINO # 002 ISMS **Administrátorská příručka bezpečnosti informací**.

### 11.2. Řízení přístupu k síti

ICT oddělení poskytuje uživatelům přístup do sítě. Uživatelé sítě v jakékoli pozici hierarchie IS mají vždy přidělen konkrétní účet, přihlašovací jméno, oprávnění k přístupu na požadovanou úroveň a heslo. Heslo je nutné změnit po prvním přihlášení. Vzdálený přístup zaměstnanců do vnitřní sítě společnosti je umožněn prostřednictvím VPN spojení (vždy s vynucenou dvoufaktorovou autentizací).

Více informací viz PALASINO # 002A ISMS **Administrátorská příručka bezpečnosti informací**.

### 11.3. Řízení přístupu k operačním systémům

Kontrolu přístupu k operačním systémům poskytuje systémová služba Microsoft Active Directory a Microsoft365 Entra

Účet správce systému lze použít pouze pro systémový management.

Některé aplikace používají vlastní řízení přístupu k informacím v nich zpracovávaných.

### 11.4. Řízení přístupu k aplikacím

Některé aplikace používají své vlastní řízení přístupu (např. NEON, atd.). Tato aplikační práva mohou být v omezené míře v rozporu s nastavenými politikami přístupových práv k operačnímu systému, zejména se zajištěním několika-úrovňového přístupu (zejména u klasifikovaných informací) pro jednotlivé uživatele/funkce.

Je doporučeno využívání správce hesel např. Pleasant Password Manager

.Je výslovně zakázáno pro vyjmenované aplikace využívat systém autologon.

- Operační systém
- VPN
- VPN zákazníci
- Přihlášení na provozní servery pomocí terminálových služeb

## 12. Řízení fyzického přístupu

Veškeré neveřejné a veřejné prostory kasina, včetně serveroven, ve kterých jsou provozovány klíčové technologie IS Palasino, a kde je možný přístup k těmto prostředkům jsou navrhovány a uspořádány tak, aby splňovaly níže uvedené doporučené parametry fyzického zabezpečení. Pro zajištění bezpečnosti v serverovnách a kamerových serverovnách monitorovaných v souladu s ISO 27001 byla implementována procedura *ADM 39 Kontrola režimových pracovišť a řízení fyzického přístupu (0427)*, která popisuje procedury a postupy, které zahrnují fyzické zabezpečení, monitorování a kontrolu přístupu.

Níže jsou uvedeny klíčové kroky a doporučení pro fyzické umístění a zabezpečení.

- Prostory se zařízeními IS Palasino musí ležet mimo zátopovou oblast tzv. stoleté vody.
- Prostory se zařízeními IS Palasino musí být nepřetržitě fyzicky chráněny za použití bezpečnostních perimetrů (bariéry jako například zdi atd.).
- Vstup do těchto prostor musí být řízen, tzn. umožněn pouze oprávněným osobám.
- Teplota uvnitř místnosti musí být zajištěna v rozmezí od 18 °C do 26 °C a nepřetržitě monitorována.
- Relativní vlhkost musí být v rozmezí 35 % - 65 %.
- Místnost musí být vybavena zařízeními na ochranu proti škodám způsobeným:
  - lidským faktorem.
  - povětrnostními podmínkami.
  - vodou.
  - požárem.
  - prachem – musí být zajištěna úklidová služba. Způsob provádění úklidových prací by měl být zajištěn tak, aby probíhal v souladu s Politikou bezpečnosti informací Palasino.
- Zařízení musí být chráněno před selháním primárního napájení 230V/50Hz „bezvýpadkovými“ záložními zdroji napájení UPS.
- Přívod elektřiny musí být samostatně jištěný. V místě se předpokládá vyvedený zemnicí bod pro připojení ochranných vodičů z jednotlivých racků.

Veškeré ostatní postupy viz procedura *ADM 39 Kontrola režimových pracovišť a řízení fyzického přístupu (0427)*.

## 13. Akvizice, vývoj a údržba informačních systémů

### 13.1. Politika bezpečného vývoje

Organizace neprovádí vlastní vývoj, akvizice provozovaného systému NEON. je systematicky řízena, jsou prováděny testy jednotlivých nových release před aplikací do produkčního prostředí.

Realizované změny jsou popsány řízením změn a dokumentovány v papírové Servisní knize oprav NEON..

Bezpečnostní požadavky na informační systém stanovuje rovněž bezpečnostní fórum (CARCOM), které musí být zapojeno do procesu výběru a implementace informačních systémů.

Specifikace informačního systému.

Vyhodnocení možných alternativ (výběrové řízení).

Funkční (technická) specifikace (v případě dodavatelského vývoje).

Výsledky přijímacích testů (v případě dodavatelského vývoje).

Bezpečnostní dokumentace předaná do informačního systému.

#### Proces bezpečného vývoje

Proces bezpečného vývoje pomáhá ICT Manažerovi řešit bezpečnostní rizika. Proces je rozdělen do čtyř hlavních částí:

Funkční a bezpečnostní potřeby.

Hrozby a mimořádné události, které mohou mít vliv na systém.

Řešení bezpečnosti vedoucí ke snížení rizik.

Zbytková rizika.

Systémy zpracování dat s nutností zajištění jejich integrity (zejména legislativní a jiné zveřejněné dokumenty, smlouvy a personální agenda) musí zahrnovat mechanismy pro provedení technické kontroly vstupních dat a kontrolu přístupu a provozu, což je dokumentováno např. ve Statement of Work pro NEON systém.

Databázové systémy musí zajistit, že všechny datové změny udržují integritu informací. Tam, kde to je relevantní, může být použita technická kontrola výstupních dat.

### 13.2. Kryptografické kontroly

Šifrovací systémy a technologie musí být použity k ochraně informací, které jsou považovány za rizikové (chráněné) a pro které jiná řešení neposkytují dostatečnou ochranu.

Šifrování se používá na ochranu chráněných informací. Kryptografická řešení jsou v PALASINO standardizována. – kompletní informace jsou uvedeny v **Uživatelské příručce bezpečnosti informací**.

Odpovědnost za správu šifrovacích klíčů, včetně využití metod obnovy šifrovaných informací v případě ztráty, poškození nebo prozrazení klíčů je v gesci Managera ICT .

### 13.3. Bezpečnost při testování nových funkcí IS

Testovací prostředí mohou být vytvořena pouze s vědomím ICT oddělení, které musí mít plnou kontrolu na úrovni správy systému. Testovací prostředí je odděleno od zpracovávání interních produkčních dat. Testování může probíhat se vzorkem starších produkčních dat, které musí být zabezpečeny pro úroveň klasifikace chráněné

Preferuje se použití fiktivních údajů, využití labu „playground“ uživatelů poskytnutých MF pro účely testování. Pokud je z důvodu účinnosti nevyhnutelné použít produkční data, je nutné zajistit, aby testovací prostředí bylo v souladu s požadavky Politiky bezpečnosti informací a se související dokumentací.

## 14. Pravidla využití AI

Pro využití AI v denní práci a praxi platí pravidla nastavené v proceduře ADM 40 Pravidla pro využití AI ve společnosti PALASINO (0427).

## 15. Management bezpečnostních incidentů

### 15.1. Hlášení bezpečnostních událostí a slabin

Bezpečnostní incident a bezpečnostní slabiny jsou reportovány, zaznamenávány a zpracovávány.

#### HLÁŠENÍ INCIDENTŮ IT

Veškeré chyby zjištěné v nastavení nebo zabezpečení systému musí být nahlášeny příslušnému správci systému (evidence incidentu je zadávána pomocí aplikace TASKPOOL HELPDESK a na email ISO@PALASINO.cz), aby bylo možné přijmout opatření k prošetření a vyřešení problému včetně zodpovědnosti a termínu realizace.

Pokud se o porušení tohoto postupu dozví správce systému, je oprávněn přijmout přiměřená opatření k zavedení a uplatnění tohoto postupu a k zabezpečení systému. Správce systému může dočasně pozastavit přístupová práva, je-li přesvědčen, že je to nutné nebo vhodné k zachování integrity počítačového systému nebo sítě.

Od uživatelů se očekává, že budou na vyzvání spolupracovat se správci systému při jakémkoliv vyšetřování zneužití systému nebo možného zneužití systému. Uživatelé jsou vyzýváni k tomu, aby nahlásili podezření ze zneužití, zejména jakékoliv poškození nebo problémy s jejich soubory.

### 15.2. Příklady bezpečnostních incidentů

Následující činnosti představují příklady dříve popsaných nebo dalších činností, které jsou zakázané a mohou vést k disciplinárnímu řízení. Tento seznam není kompletní a nepředstavuje všechny možnosti porušení.

Příklady porušení pravidel používání e-mailu a Internetu:

- posílání nebo zveřejňování diskriminačních, obtěžujících nebo vyhrožujících zpráv nebo obrázků;
- využívání času a zdrojů organizace pro osobní účely;
- získání, používání nebo prozrazení kódu nebo hesla někoho jiného bez jeho svolení;
- kopírování, pirátské kopírování nebo stahování softwaru a elektronických souborů bez povolení;
- posílání nebo zveřejňování důvěrného materiálu, obchodních tajemství nebo chráněných informací mimo společnost;
- porušování autorských práv;
- nedodržování licenčních smluv;
- účast na neoprávněných transakcích, které mohou vést ke vzniku nákladů pro společnost nebo iniciovat nežádoucí Internetové služby a přenosy;
- posílání nebo zveřejňování zpráv nebo materiálů, které by mohly poškodit image nebo dobrou pověst společnosti;
- posílání nebo zveřejňování zpráv, které pomlouvají nebo očerňují jiné osoby;
- pokus o vniknutí do počítačového systému jiné organizace nebo osoby;
- odmítnutí poskytnout součinnost při bezpečnostním vyšetřování;
- posílání nebo zveřejňování řetězových dopisů, žádostí o pomoc nebo inzerátů, které nesouvisí s obchodními účely nebo činnostmi;
- používání internetu pro politické věci nebo činnosti, náboženskou činnost nebo jakoukoliv formu hazardních her;
- ohrožování bezpečnosti firemního systému elektronické komunikace;

- posílání nebo zveřejňování zpráv, které shazují produkty nebo služby jiné společnosti;
- prezentování osobních názorů v roli zástupce společnosti;
- posílání anonymních e-mailových zpráv; resp.
- zapojení se jakékoliv nezákonné činnosti.

### 15.3. Správa bezpečnostních incidentů a proces zlepšování

#### Odpovědnosti a postupy

IT Security Manager je primárním kontaktem pro řešení všech bezpečnostních aspektů k zajištění analýzy incidentů.

#### Ponaučení z bezpečnostních incidentů

V rámci rozsahu informačního systému pro reportování incidentů IT Security Manager monitoruje a vyhodnocuje informace o nahlášených incidentech jemu spravované oblasti, které mu slouží k vyhodnocování, pro účely statistiky a pro návrh adekvátních opatření k budoucí eliminaci prodělaných incidentů.

#### Shromažďování evidence incidentů

Zachování důkazů v případě podezření na nelegální činnosti může provádět pouze vedení společnosti. V případě takového incidentu se organizační jednotka PALASINO, která se podílí na vyšetřování, musí obrátit na bezpečnostní fórum pro další pokyny. Sama nesmí zahájit vlastní vyšetřování a shromažďování důkazů (možné poškození důkazů).

V případě podezření na trestný čin v souvislosti s provozem zahrnující informační systém musí PALASINO kontaktovat policii a musí se řídit jejími pokyny, zejména v oblasti identifikace, zajištění a udržení všech důkazů.

## 16. Management kontinuity

### 16.1. Bezpečnostní aspekty řízení kontinuity

Zajištění procesů kontinuity je v gesci vedení PALASINO. Formální odpovědnost za kontinuitu informačního systému a za jeho bezpečnost je přiřazena bezpečnostnímu fóru.

Platí:

Identifikovaná rizika ve vztahu k procesům informačního systému musí být adekvátně chráněna proti možnému přerušení či selhání procesů a návazných procesů.

Pro každý rizikový proces musí být definován maximální tolerovatelný čas nedostupnosti a během této doby je nutné zajistit návrat do stavu před selháním nebo nehodou a zajistit tak kontinuitu procesů.

Za identifikaci rizikových procesů je odpovědné bezpečnostní fórum, které spolupracuje v této záležitosti s individuálními vlastníky aktiv.

Údržba plánů kontinuity je základním cílem havarijního plánování, tj. havarijních plánů, plánů kontinuity a plánů obnovy. Havarijní plány obsahují podrobný popis postupů a opatření v případě havárií informačního systému včetně definice odpovědností a povinností.

Potřeba zajištění kontinuity záleží na správném určení rizik přerušení každého specifického procesu, na hodnotě PALASINO aktiv a na vlivu či dopadu selhání specifických komponent informačního systému. Opatření a prostředky používané k ochraně těchto aktiv musí být srovnatelné s jejich hodnotou, a proto je žádoucí:

- co nejpřesnější vyjádření hodnoty aktiv v případě jeho ztráty, včetně odhadu nákladů na jeho obnovení, znovupořízení či opětovné uvedení do provozu atd.;
- kvalitativní posouzení a stanovení priorit obnovy.

### 16.2. Testování, údržba a přezkoumání plánů kontinuity

Účinnost havarijního plánu se ověřuje jednak teoretickou simulací havárie a jednak praktickým testováním, kde je to možné, popř. je to vhodné ve spojení s kritickými procesy. Údržba, přezkum, aktualizace a změny v plánu jsou v gesci IT Security managera, který musí úzce spolupracovat s příslušnými zaměstnanci – manažery a vlastníky informačních aktiv, atd. ICT BCM testy jsou plánovány a hodnoceny každoročně a jejich výsledky jsou projednány na bezpečnostním fóru.

Detaily řeší **Administrátorská příručka bezpečnosti informací**

## 17. Shoda s bezpečnostními požadavky

Statutární, regulační, právní a smluvní závazky s ohledem na bezpečnosti informací musí být plněny.

### 17.1. Ochrana duševního vlastnictví

Autorská práva třetích osob musí být respektována. Autorská práva společnosti PALASINO musí být chráněna. Každý uživatel si musí být jasně vědom ochrany autorských práv. V případě potřeby musí být autorská práva společnosti PALASINO právně vymáhána (např. podáváním žádostí o patenty).

Software je pořízován a smí být užíván pouze v rámci licenčních předpisů a pouze v souladu s platnými předpisy PALASINO. Podrobnosti jsou uvedeny v **Uživatelské příručce bezpečnosti informací** a v **Administrátorské příručce bezpečnosti informací**, kde jsou i uvedeny definice pro nakládání s povoleným a zakázaným software.

Každý nákup softwarového produktu vede k nutnosti evidence licencí. Veškerý software nainstalovaný na hardware musí být řádně ověřen. Aby se předešlo jakémukoliv licenčnímu porušování, tak je pravidelně prováděn softwarový audit formou kontroly účetní evidence SW v majetku a na základě faktur za využívání SW předplatného.

### 17.2. Ochrana dat a osobních údajů

Při sběru, zpracování a použití osobních údajů jsou dodržovány místní právní a organizační předpisy v souladu s GDPR a zákonem 110/2019 Sb.

Sběr dat, zpracování a využívání osobních údajů může být provedeno pouze, pokud je v souladu s těmito zásadami:

Pouze pro služební účely.

Pouze za předpokladu informování dotčené osoby s výjimkou veřejně dostupných dat o osobě.

Zajištění práv námitky a žádost o opravu, jakož i právo na přístup k osobním údajům pro zúčastněné osoby ve smyslu GDPR.

Za výklad a procesy GDPR odpovídá Pověřenec pro ochranu osobních údajů.

### 17.3. Dodržování bezpečnostních politik a standardů, technická shoda

Bezpečnostní fórum v rámci svých povinností provádí kontrolu dodržování a implementace bezpečnostních politik a standardů. Návrhy na změny bezpečnostní dokumentace předkládá IT Security Manager.

Vedení společnosti PALASINO je odpovědné za vytváření podmínek pro plnění a dodržování Politiky bezpečnosti informací.

IT Security Manager je povinen zajistit, že vlastníci IS a aplikací se podílí na dodržování Politiky bezpečnosti informací včetně účasti na jejím pravidelném přezkoumání s ohledem na:

Úroveň implementace Politiky bezpečnosti informací.

Účinnost přijatých bezpečnostních opatření včetně zohlednění kontextu nových hrozeb.

## 17.4. Hlediska auditu informačního systému

Řízení auditu informačního systému

Pro audit systému jsou nutná alespoň tato opatření:

Auditorské požadavky a rozsah auditu musí být odsouhlaseny vedením společnosti PALASINO.

Auditoři mají obvykle přiřazen přístup pouze pro čtení. Prověřování přístupových oprávnění jiných než pro čtení by mělo být prováděno pouze na izolované kopii IS. Tyto kopie musí být vymazány po ukončení auditu.

Všechny postupy, požadavky a povinnosti musí být zdokumentovány.

Ochrana nástrojů auditu informačních systémů

Systémové nástroje auditu a výstupní data auditu musí být chráněna proti neoprávněnému přístupu a zneužití. Tyto auditní nástroje by měly být odděleny od vývojových a provozních systémů.

## 18. Bezpečnost informací při přístupu externích dodavatelů a třetích stran

Cílem této směrnice je zajistit, že při poskytování přístupu dodavatelům a třetím stranám ke zmíněným aktivům organizace jsou vhodným způsobem řízeny požadavky bezpečnosti informací a jsou přehledně přiřazeny odpovědnosti odpovídající požadavkům normy ISO27001

### 18.1. Identifikace aktiv a přístupů

Palasino identifikuje aktiva (data, systémy, prostory), ke kterým bude umožněn přístup dodavatelům/třetím stranám v rámci analýzy rizik.

Pro každé aktivum stanoví úroveň a rozsah přístupu (čtení, zápis, správa apod.) a příslušná bezpečnostní opatření (např. šifrování, omezení přístupů).

Přístup je poskytován pouze na základě schválených žádostí a definovaných rolí.

### 18.2. Dokumentace a odsouhlasení požadavků s dodavateli

Požadavky bezpečnosti informací jsou vždy zahrnuty do smluv, rámcových dohod, příloh nebo SLA smluv s dodavateli. Tyto požadavky jsou dokumentovány a formálně odsouhlaseny oběma stranami. Dodavatel je jednoznačně seznámen s povinnostmi i důsledky nedodržení (např. sankce, ukončení spolupráce). Je nutné dodržet, před zahájením spolupráce, podepsání základní smlouva a, dle způsobu přístupu, NDA, DPA,. Dále pak je nutné zajistit s dodavatelem seznámení s politikami bezpečnosti ISO 002A ISO002B, ISO003 a politiku desatera a jejich závazek za seznámení s jejich zaměstnanci.

### 18.3. Přiřazení odpovědností

Palasino jmenuje interně osobu zodpovědnou, nebo zplnomocněnou, za správu vztahu s dodavatelem a dohled nad plněním požadavků bezpečnosti informací. Dodavatel je povinen jmenovat osobu odpovědnou za bezpečnost informací při poskytování služeb organizaci. Mezi klíčové odpovědnosti patří:

- Dodržování stanovených bezpečnostních opatření. Seznámení s politikami bezpečnosti.
- Pravidelná komunikace o plnění požadavků a hlášení případných incidentů.
- Spolupráce při interních nebo externích auditech.
- Odpovědnost za proškolení svých zaměstnanců s přístupem k aktivům organizace.
- Plnění požadavků platné legislativy.

### 18.4. Pravidelné kontroly a audit

Palasino pravidelně každé pololetí hodnotí dodržování bezpečnostních požadavků ze strany dodavatele.

Pravidelně provádí audity a kontroly dle smluvních podmínek a uchovává záznamy o této činnosti.

## 18.5. Ukončení přístupu a spolupráce

Při ukončení smluvního vztahu je dodavateli odebrán přístup ke všem aktivům. Dodavatel je povinen poskytnout písemné prohlášení o smazání, likvidaci nebo navrácení všech aktiv souvisejících s organizací. Organizace archivuje související dokumenty a zápisy o ukončení spolupráce.

## 18.6. Vzorové body do smlouvy/dohody

- Dodavatel se zavazuje chránit informace a aktiva dle požadavků organizace a této směrnice.
- Přístup je povolen pouze po předchozím schválení, v rozsahu nutném pro plnění smlouvy.
- Dodavatel jmenuje zodpovědnou osobu pro oblast bezpečnosti informací.
- Dodavatel neprodleně oznamuje každý bezpečnostní incident organizaci.
- Po ukončení vztahu neprodleně smaže nebo vrátí všechna aktiva Palasina.

**Příloha č. 1****Seznam právních předpisů pro Palasino Group, a.s.**

Níže je předkládán seznam relevantních právních předpisů, kterými se musí společnost Palasino Group, a.s. řídit při své činnosti. Seznam je pro lepší přehlednost rozdělen do jednotlivých kategorií podle předmětu právní úpravy.

**Hazardní hry**

1	Zákon č. 186/2016 Sb., o hazardních hrách
2	Vyhláška č. 208/2017 Sb., kterou se stanoví rozsah technických parametrů, jejichž prostřednictvím jsou provozovány hazardní hry, požadavků na ochranu a uchovávání herních a finančních dat a jejich technické parametry
3	Vyhláška č. 433/2021 Sb., o výstupních dokumentech v oblasti hazardních her
4	Vyhláška č. 10/2019 Sb., o způsobu oznamování a zasílání informací a přenosu dat provozovatelem hazardních her, rozsahu přenášených dat a jiných technických parametrech přenosu dat
5	Zákon č. 188/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o hazardních hrách a zákona o dani z hazardních her
6	<u>Obecně závazná vyhláška Obce Česká Kubice č. 12017 o regulaci hazardních her</u>
7	<u>Obecně závazná vyhláška obce Chvalovice č. 2/2016 o omezení provozování loterií a jiných podobných her</u>
8	Zákon č. 89/2012 Sb., občanský zákoník
9	Zákon č. 349/2023 Sb., Zákon, kterým se mění některé zákony v souvislosti s konsolidací veřejných rozpočtů a s ním spojeným požadavkům související legislativy

**Směnárství**

1	Zákon č. 277/2013 Sb., o směnárenské činnosti
2	Vyhláška č. 315/2013 Sb., o směnárenské činnosti
3	Zákon č. 136/2011 Sb., o oběhu bankovek a mincí

**AML**

1	Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu
2	Vyhláška č. 67/2018 Sb., o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti a financování terorismu
3	Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí
4	Nařízení Evropského parlamentu a Rady (EU) 2015/847 ze dne 20. května 2015 o informacích doprovázejících převody peněžních prostředků a o zrušení nařízení (ES) č. 1781/2006
5	Zákon č. 254/2004 Sb., o omezení plateb v hotovosti

**Ubytování**

1	Zákon č. 89/2012 Sb., občanský zákoník - § 1852-1867 Dočasné užívání ubytovacího zařízení a jiné rekreační služby
2	Zákon č. 89/2012 Sb., občanský zákoník - § 2326-2331 Ubytování
3	Zákon č. 89/2012 Sb., občanský zákoník - § 1816 Účinky odstoupení
4	Zákon č. 89/2012 Sb., občanský zákoník - § 1837 Nemožnost odstoupit od smlouvy
5	Zákon č. 89/2012 Sb., občanský zákoník - § 2946 - § 2949 Škoda na vnesené věci – prostory ubytování
6	Nařízení vlády č. 278/2008 Sb., o obsahových náplních jednotlivých živností - Příloha č. 4 Obsahová náplň živnosti volné podle jednotlivých oborů činností – 55. Ubytovací služby
7	Zákon č. 586/1992 Sb., o daních z příjmů
8	Zákon České národní rady č. 565/1990 Sb., o místních poplatcích
9	Obecně závazná vyhláška obce Dolní Dvořiště č. 1/2019 o místních poplatcích
10	Obecně závazná vyhláška obce Chvalovice č. 2/2019 o místním poplatku z pobytu
11	Zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky
12	Vyhláška č. 501/2006 Sb., o obecných požadavcích na využívání území
13	Vyhláška č. 268/2009 Sb., o technických požadavcích na stavby

**Restaurace**

1	Nařízení Evropského parlamentu a Rady (ES) č. 178/2002, kterým se stanoví obecné zásady a požadavky potravinového práva, zřizuje se Evropský úřad pro bezpečnost potravin a stanoví postupy týkající se bezpečnosti potravin
2	Nařízení Evropského Parlamentu a Rady (ES) č. 853/2004 ze dne 29. dubna 2004, kterým se stanoví zvláštní hygienická pravidla pro potraviny živočišného původu
3	Vyhláška č. 137/2004 Sb., o hygienických požadavcích na stravovací služby a o zásadách osobní a provozní hygieny při činnostech epidemiologicky závažných, v platném znění
4	Vyhláška č. 490/2000 Sb., o rozsahu znalostí a dalších podmínkách k získání odborné způsobilosti v některých oborech ochrany veřejného zdraví
5	Vyhláška č. 366/2005 Sb., o požadavcích vztahujících se na některé zmrazené potraviny
6	Vyhláška č. 157/2003 Sb., kterou se stanoví požadavky pro čerstvé ovoce a čerstvou zeleninu, zpracované ovoce a zpracovanou zeleninu, suché skořápkové plody, houby, brambory a výrobky z nich, jakož i další způsoby jejich označování

**Přeprava osob**

1	Zákon č. 89/2012 Sb., občanský zákoník - § 2550-2554 Přeprava osoby
2	Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu)
3	Zákon č. 13/1997 Sb., o pozemních komunikacích
4	Zákon č. 111/1994 Sb., o silniční dopravě
5	Zákon č. 168/1999 Sb., o pojištění odpovědnosti za škodu způsobenou provozem vozidla
6	Vyhláška č. 435/2012 Sb., o užívání pozemních komunikací zpoplatněných časovým poplatkem
7	Vyhláška č. 470/2012 Sb., o užívání pozemních komunikací zpoplatněných mýtným
8	Vyhláška č. 522/2006 Sb., o státním odborném dozoru a kontrolách v silniční dopravě
9	Vyhláška č. 104/1997 Sb., kterou se provádí zákon o pozemních komunikacích
10	Vyhláška č. 478/2000 Sb., kterou se provádí zákon o silniční dopravě
11	Nařízení vlády č. 589/2006 Sb., kterým se stanoví odchylná úprava pracovní doby a doby odpočinku zaměstnanců v dopravě
12	Nařízení vlády č. 168/2002 Sb., kterým se stanoví způsob organizace práce a pracovních postupů, které je zaměstnavatel povinen zajistit při provozování dopravy dopravními prostředky
13	Nařízení vlády č. 278/2008 Sb., o obsahových náplních jednotlivých živností
14	Zákon o ochraně oznamovatelů č. 171/2023 Sb.

**Kosmetické služby**

1	Nařízení Evropského parlamentu a Rady (ES) č. 1223/2009 ze dne 30. listopadu 2009 o kosmetických přípravcích
2	Zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů

**Prodej kvasného, konzumního lihu a lihovin**

1	Zákon č. 307/2013 Sb., o povinném značení lihu
2	Zákon č. 353/2003 Sb., o spotřebních daních

3	Zákon č. 61/1997 Sb., o lihu
4	Vyhláška č. 248/2018 Sb., o požadavcích na nápoje, kvasný ocet a droždí

**GDPR**

1	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
2	Zákon č. 110/2019 Sb., o zpracování osobních údajů
3	Zákon č. 480/2004 Sb., o některých službách informační společnosti
4	Zákon č. 89/2012 Sb., občanský zákoník

**Zaměstnanost**

1	Zákon č. 262/2006 Sb., zákoník práce
2	Zákon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci
3	Zákon č. 251/2005 Sb., o inspekci práce
4	Nařízení vlády č. 567/2006 Sb., o minimální mzdě
5	Zákon č. 2/1991 Sb., o kolektivním vyjednávání
6	Nařízení vlády č. 101/2005 Sb., o podrobnějších požadavcích na pracoviště a pracovní prostředí
7	Nařízení vlády č. 361/2007 Sb., kterým se stanoví podmínky ochrany zdraví při práci
8	Nařízení vlády č. 589/2006 Sb., kterým se stanoví odchylná úprava pracovní doby a doby odpočinku zaměstnanců v dopravě
9	Nařízení vlády č. 168/2002 Sb., kterým se stanoví způsob organizace práce a pracovních postupů, které je zaměstnavatel povinen zajistit při provozování dopravy dopravními prostředky
10	Vyhláška č. 180/2015 Sb., o pracích a pracovištích, které jsou zakázány těhotným zaměstnankyním, zaměstnankyním, které kojí, a zaměstnankyním-matkám do konce devátého měsíce po porodu, o pracích a pracovištích, které jsou zakázány mladistvým zaměstnancům, a o podmínkách, za nichž mohou mladiství zaměstnanci výjimečně tyto práce konat z důvodu přípravy na povolání (vyhláška o zakázaných pracích a pracovištích)
11	Nařízení vlády č. 590/2006 Sb., kterým se stanoví okruh a rozsah jiných důležitých osobních překážek v práci
12	Nařízení vlády č. 201/2010 Sb., o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu

**Ostatní**

1	Zákon č. 563/1991 Sb., o účetnictví
2	Vyhláška č. 500/2002 Sb., kterou se provádějí některá ustanovení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, pro účetní jednotky, které jsou podnikateli účtujícími v soustavě podvojného účetnictví
3	Zákon č. 586/1992, o daních z příjmů
4	Zákon č. 16/1993 Sb. České národní rady, o dani silniční
5	Zákon č. 235/2004, o dani z přidané hodnoty
6	Zákon č. 187/2006 Sb., o nemocenském pojištění
7	Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění
8	Zákon č. 592/1992 Sb., o pojistném na veřejné zdravotní pojištění
9	Zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti
10	Zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon)
11	Zákon č. 40/1995 Sb., o regulaci reklamy
12	Zákon č. 634/1992 Sb., o ochraně spotřebitele
13	Zákon č. 65/2017 Sb., o ochraně zdraví před škodlivými účinky návykových látek
14	Zákon č. 64/1986 Sb., o České obchodní inspekci
15	Zákon č. 198/2009 Sb., antidiskriminační zákon
16	Zákon č. 90/2012 Sb., o obchodních korporacích
17	Zákon č. 258/2000 Sb., o ochraně veřejného zdraví
18	Zákon č. 526/1990 Sb., o cenách
19	Zákon č. 133/1985 Sb., o požární ochraně
20	Zákon č. 143/2001 Sb., o ochraně hospodářské soutěže
21	Nařízení č. 23/2008 Sb., o technických podmínkách požární ochrany staveb
22	Zákon č. 338/1992 Sb., o dani z nemovitých věcí
23	Zákon č. 348/2005 Sb., o rozhlasových a televizních poplatcích

<b>24</b>	Zákon č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon)
<b>25</b>	Vyhláška č. 268/2009 Sb., o technických požadavcích na stavby
<b>26</b>	Zákon č. 264/2025 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
<b>27</b>	Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
<b>28</b>	ČSN EN ISO/IEC 27001:2023 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky
<b>29</b>	ČSN ISO/IEC 27004:2018 Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Monitorování, měření, analýza a hodnocení
<b>30</b>	ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks
<b>31</b>	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
<b>32</b>	ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls