SwissLife
Select

Platná od 1. 5. 2016

Bezpečnostní politika

Deklarace

1. Předmět a účel

Předmětem této Bezpečnostní politiky je definovat celkový rámec a pravidla pro bezpečné nakládání s informacemi v jakékoliv formě v rámci Swiss Life Select, zejména pak v prostředí informačního systému Swiss Life Select a při práci s výpočetní technikou.

Swiss Life Select poskytuje širokému spektru ijgclrâ služby privátního finančního poradenství spojené s finanční analýzou, optimalizací atd. V rámci těchto činností přicházíme do styku a nakládáme s řadou citlivých informací, jako jsou osobní údaje klientů, informace o jejich finanční situaci apod.

1.1 Prohlášení vedení Swiss Life Select

Důsledné zajištění bezpečnosti těchto i dalších informací v prostředí Swiss Life Select tak, abychom dostáli svým závazkům vůči našim klientům, obchodním partnerům a dalším subjektům, stejně tak jako závazkům vyplývajícím z platné legislativy, je jedním z našich hlavních cílů.

Vedení Swiss Life Select si uvědomuje, že existují určitá rizika bezpečnosti informací, a je proto nutné systematicky vytvářet takové prostředí, které povede k jejich účinné a efektivní eliminaci. Vedení společnosti deklaruje touto Bezpečnostní politikou svou strategii a podporu trvalého zajišťování informační bezpečnosti jako nedílné součásti všech řídicích procesů Swiss Life Select.

1.2 Cíle informační bezpečnosti

Mezi základní cíle bezpečnosti informací Swiss Life Select patří:

- zajištění potřebné úrovně důvěrnosti veškerých informací klientů,
- zachování potřebné dostupnosti informací a služeb informačního systému,
- zajištění bezpečného a oprávněného přístupu k informačnímu systému a k informacím v rámci informačního systému,
- zajištění všech definovaných atributů bezpečnosti (důvěrnosti, dostupnosti, integrity),
- stanovení odpovědnosti za činnost uživatelů a dalších rolí v informačním systému,
- řízení rizik s cílem efektivních bezpečnostních opatření,
- zajištění kontinuity a havarijního plánování informačního systému,
- dodržování požadavků právních předpisů, technických norem a interních předpisů.

Bezpečnost informací Swiss Life Select je postavena na třech základních principech, a to na zajištění důvěrnosti, integrity a dostupnosti informací v rámci Swiss Life Select.

- Důvěrnost znamená zajištění přístupu k informacím pouze autorizovanými uživateli s potřebným oprávněním.
- Integrita obnáší zajištění správnosti a úplnosti informací a procesů.
- Dostupnost zajišťuje, že oprávnění uživatelé mají přístup k informacím a souvisejícím aktivům informačního systému tehdy, když je potřebují nebo když jsou jimi požadovány.

1.3 Působnost (rozsah platnosti)

Bezpečnostní politika a další na ni návazné interní dokumenty jsou platné v rozsahu celé společnosti, tzn. vztahují se h_i l_ back-office* r_i g l_ hcblmrjgtă poradenská centra (front-office).

Bezpečnostní politika je závazným dokumentem, se kterým musí být prokazatelně seznámeni všichni zaměstnanci a pracovníci Swiss Life Select minimálně na úrovni Bezpečnostní příručky pro danou oblast (back-office nebo front-office).

2. Východiska bezpečnostní politiky Swiss Life Select

Výchozími právními předpisy pro řešení problematiky bezpečnosti jsou:

- zákon č. 101/2000 Sb., o ochraně osobních údajů;
- zákon č. 363/1999 Sb., o pojišťovnictví;
- zákon č. 38/2004 Sb., o pojišťovacích zprostředkovatelích;
- zákon č. 227/2000 Sb., o elektronickém podpisu;
- zákon č. 121/2000 Sb., o právu autorském;
- zákon č. 480/2004 Sb., o některých službách informační společnosti;
- zákon č. 89/2012 Sb., občanský zákoník;
- zákon č. 499/2004 Sb., o archivnictví a spisové službě;
- zákon č. 40/2009 Sb., trestní zákoník;
- zákon č. 256/2004 Sb., o podnikání na kapitálovém trhu;

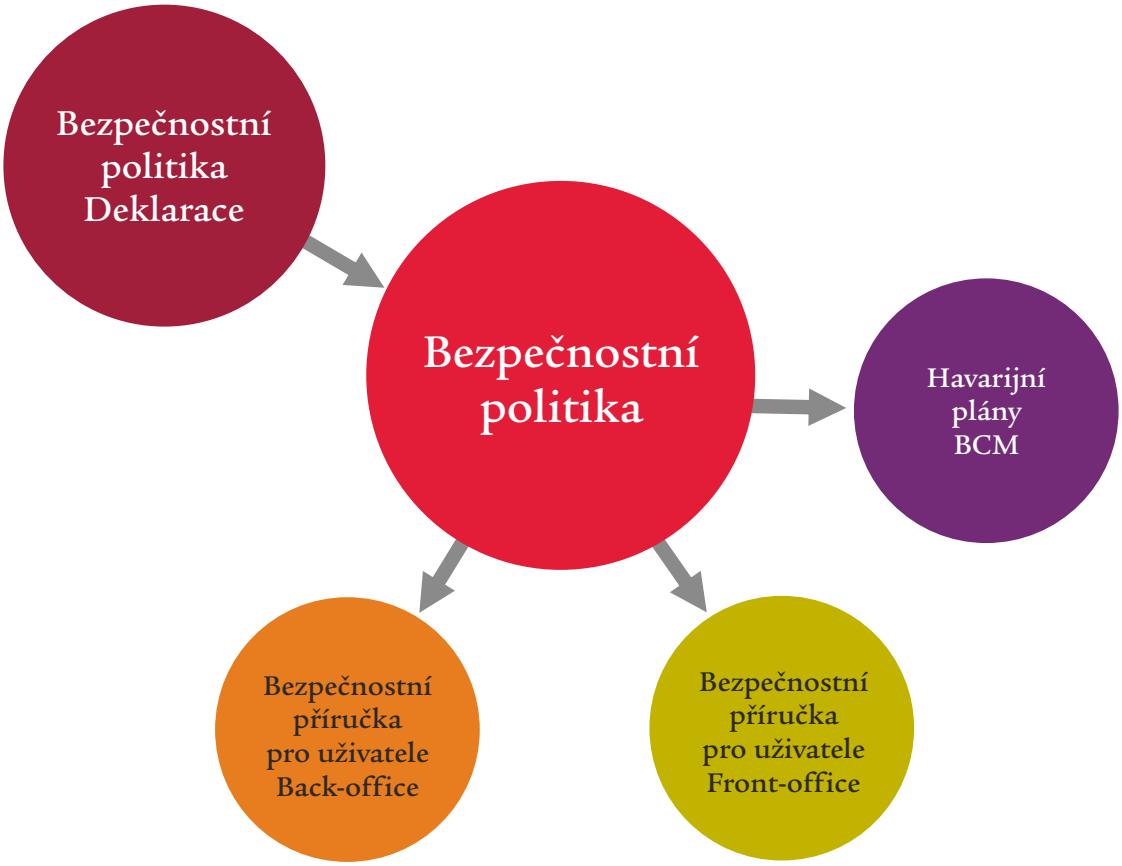
v platném znění a další relevantní právní předpisy.

Oblast bezpečnosti informací je v prostředí Swiss Life Select dále řešena v souladu se standardy ISO/IEC řady 27000, zejména ISO/IEC 27002, se zohledněním dalších standardů a metodik z oblasti informačních a komunikačních technologií jako jsou například ISO/IEC 20000, ITIL, CoBIT a další.

3. Rámec řešení bezpečnosti informací Swiss Life Select

3.1 Politiky informační bezpečnosti (Information Security Policies)

V rámci Swiss Life Select je bezpečnostní dokumentace tvořena následujícími dokumenty:



Deklarace bezpečnostní politiky je určena všem zaměstnancům a pracovníkům Swiss Life Select, případně i dalším subjektům ve vztahu k Swiss Life Select. Obsahuje základní rámcový popis systému řízení bezpečnosti informačních a komunikačních technologií ve Swiss Life Select.

Dokument Bezpečnostní politika (plná verze) je primárně určena oddělení IT a vedoucím zaměstnancům a pracovníkům.

Řadoví uživatelé jsou s hlavními bezpečnostními pravidly, které se na ně bezprostředně vztahují, seznamováni formou Bezpečnostních příruček, jejichž obsahem je souhrn těch nejdůležitějších bezpečnostních informací vztahujících se na běžné uživatele informačního systému.

Havarijní plány jsou určeny především oddělení IT jako podpora pro zvládání výpadků infrastruktury informačních a komunikačních technologií ve Swiss Life Select.

3.2 Organizace bezpečnosti (Organization of Information Security)

Každá osoba v rámci Swiss Life Select, která využívá výpočetní techniku a má přístup k informačnímu systému Swiss Life Select, má přidělenu určitou bezpečnostní roli, ke které náleží určitá odpovědnost za zajištění bezpečnosti a určité pravomoci.

- Koncepční řešení informační bezpečnosti provádí oddělení IT.
- Prosazování informační bezpečnosti, kontrolu dodržování zásad informační bezpečnosti provádí bezpečnostní manažer.
- Nastavení a správu jednotlivých bezpečnostních opatření zajišťují IT administrátoři.
- Za implementaci jednotlivých zásad bezpečnosti informací do praxe jsou odpovědni příslušní vedoucí zaměstnanci a pracovníci Swiss Life Select.
- Jednotlivé role mají jasně vymezené pravomoci a jsou určeny nedovolené souběhy daných rolí.

V rámci Swiss Life Select je přijata a uplatňována politika pro používání a zabezpečení mobilních zařízení a pro vzdálený přístup a práci v informačním systému Swiss Life Select.

3.3 Bezpečnost lidských zdrojů (Human Resource Security)

Každý zaměstnanec a/nebo pracovník Swiss Life Select je v rámci vstupního školení a přidělení přístupových práv k informačnímu systému prokazatelně seznámen s bezpečnostní politikou Swiss Life Select a svými povinnostmi. V rámci periodických školení je pak dále vzděláván v oblasti bezpečnosti informací. Dostatečné bezpečnostní povědomí všech uživatelů informačního systému Swiss Life Select je jednou z klíčových podmínek pro udržení potřebné úrovně bezpečnosti.

Zaměstnanci a pracovníci Swiss Life Select jsou seznámeni se skutečností, že nedodržení bezpečnostních zásad může být kvalifikováno jako porušení pracovní kázně a/nebo smluvní spolupráce a v některých případech i jako přestupek nebo trestný čin.

3.4 Klasifikace a řízení aktiv (Asset Management)

Pro všechna aktiva v rámci informačního systému Swiss Life Select (včetně informačních aktiv, tj. agendy, spisy atd.) je stanoven vlastník, který je odpovědný za ohodnocení aktiva, stanovení přípustného použití a stanovení bezpečnostních parametrů. Realizace bezpečnostních opatření je v působnosti oddělení IT.

Informace Swiss Life Select jsou v rámci organizace klasifikovány a manipulovány v souladu s pro danou kategorií klasifikace určenými postupy, jako je například označování a ukládání informací, používání výměnných médií atd.

3.5 Řízení přístupu (Access Control)

Přístupová práva, jak fyzická, tak logická, k aktivům a informacím Swiss Life Select, jsou uživatelům přidělována na základě jejich pracovních rolí. Přidělení přístupových práv v rámci různých úrovní informačního systému podléhá formálnímu schvalovacímu procesu – o přidělení přístupových práv pro uživatele žádá příslušný vedoucí zaměstnanec, samotné řízení přístupu provádí oddělení administrativy. Proces řízení přístupu zahrnuje i odebrání přiístupů v určitých situacích, jako je například odchod zaměstnance. V pravidelných intervalech je prováděna revize existujících uživatelských účtů a jim přidělených oprávnění v rámci informačního systému.

3.6 Kryptografie (Cryptography)

V rámci Swiss Life Select jsou využívány různé kryptografické technologie, a to zejména za účelem zajištění přístupu uživatelů k určeným systémům a aplikacím a za účelem zajištění důvěrnosti a integrity citlivých informací, jako jsou například osobní informace klientů a know-how Swiss Life Select.

3.7 Fyzická bezpečnost a bezpečnost prostředí (Physical and Environmental Security)

Všechna aktiva jsou v rámci Swiss Life Select chráněna vhodnými režimovými opatřeními, a to zejména na úrovni zajištění fyzického přístupu k aktivům a k prvkům informačního systému. Klíčová aktiva fyzické povahy jsou chráněna v rámci vyhrazených perimetrů za použití zvýšených bezpečnostních opatření v definovaných oblastech, jako je například ochrana vůči vlivům prostředí, ochrana před nežádoucím fyzickým přístupem, provádění údržby apod.

Všichni zaměstnanci a pracovníci Swiss Life Select jsou povinni dodržovat zásady „prázdného stolu a prázdné obrazovky“ (clear desk and clear screen policy).

3.8 Bezpečnost provozu informačního systému (Operations Security)

Pro řízení, správu a monitorování aktiv v rámci informačního systému Swiss Life Select jsou vytvořeny pracovní postupy respektující bezpečnostní zásady a bezpečnostní požadavky. Pracovní postupy jsou dostupné všem dotčeným osobám a podléhají pravidelným revizím.

Na zařízeních ve vlastnictví Swiss Life Select je zakázáno instalovat a provozovat programové vybavení, které nebylo schváleno. Veškerý vývoj a testování programů probíhá na vyhrazeném testovacím prostředí odděleném od produkčních systémů.

Swiss Life Select se aktivně brání proti vlivu škodlivých programů, chybám v programech a ztrátě dat. Data jsou uložena ve vyhrazených prostorech, jsou chráněna a zálohována. Všechny zveřejněné chyby programů jsou co nejdříve opraveny. Provoz informačního systému je v odpovídající míře monitorován a záznamy jsou pravidelně vyhodnocovány.

Za řízení provozu informačního systému Swiss Life Select odpovídá vedoucí oddělení IT.

Nákup služeb potřebných pro zajištění provozu informačního systému probíhá výhradně na základě uzavřených smluv s jasně stanovenými a měřitelnými kritérii dodávek.

3.9 Bezpečnost komunikací informačního systému (Communications Security)

Zabezpečení komunikačních sítí v rámci informačního systému Swiss Life Select je nastaveno v souladu s definovanou politikou. Zejména jsou používány metody zabezpečení založené na oddělení jednotlivých částí sítě a systémů v souladu s citlivostí informací, které jsou zde ukládány a zpracovávány, a v souladu s dalšími identifikovanými riziky.

Veškeré přenosy informací v rámci sítě Swiss Life Select i mezi Swiss Life Select a externími subjekty probíhají zabezpečeným způsobem v souladu s přijatými bezpečnostními pravidly. Přenosy informací s externími subjekty jsou realizovány na základě smluvního nastavení, které obsahuje i detailní popis způsobu zabezpečení veškerých přenosů. Zpřístupňování informací Swiss Life Select externím subjektům je možné pouze na základě uzavřeného NDA (non-disclousure agreement).

3.10 Nákup, vývoj a údržba IS (System Acquisition, Development and Maintenance)

Akvizice aktiv informačního systému probíhá na základě víceletého plánu vytvářeného v minimálním horizontu jednoho roku. Součástí celého životního cyklu aktiv informačního systému Swiss Life Select a tedy i procesu akvizice je i stanovení bezpečnostních potřeb, bezpečnostních požadavků a bezpečnostních opatření v závislosti na platné bezpečnostní politice, identifikovaných rizicích a požadavcích vlastníků aktiv.

Zvláštní pozornost je věnována bezpečnosti a bezpečnostnímu monitoringu aplikací a služeb informačního systému Swiss Life Select, které jsou dostupné prostřednictvím veřejné sítě internetu.

Veškerý vývoj a změny v rámci vyvíjených systémů a aplikací jsou prováděny dle definovaného procesu, který zohledňuje zásady bezpečného vývoje a managementu změn, zejména testování v rámci odděleného prostředí, kontrolu vytvořeného kódu, případně nezávislou revizi bezpečnosti třetí stranou, a to jak u vlastního, tak u outsourcovaného vývoje.

3.11 Vztahy s dodavateli (Supplier Relationships)

U všech služeb řešených externími dodavateli jsou identifikována bezpečnostní rizika těchto služeb a jsou přijata příslušná opatření k jejich pokrytí. Přijatá bezpečnostní opatření jsou vždy projednána s dodavatelem a stávají se součástí smluvní dokumentace. Dle typu dodávané služby jsou přístupy dodavatele do sítě a k systémům Swiss Life Select vhodným způsobem monitorovány a přezkoumávány. Veškeré změny ve službách dodavatelů podléhají mj. i posouzení z hlediska možných dopadů na rizika informační bezpečnosti.

3.12 Zvládání bezpečnostních incidentů (Information Security Incident Management)

Všichni zaměstnanci a pracovníci Swiss Life Select jsou poučeni o činnostech, které mají provádět v případě podezření na výskyt bezpečnostního incidentu nebo v případě nefunkčnosti či při chybě informačního systému. Všechny podněty jsou přijaty, vyhodnoceny a archivovány. Podle závažnosti daného provozního nebo bezpečnostního incidentu jsou zahájeny procesy vedoucí k nápravě. Evidence, šetření, vyhodnocení bezpečnostních incidentů a následná nápravná preventivní opatření proti dalšímu výskytu incidentů spadají do kompetence bezpečnostního manažera.

3.13 Řízení kontinuity činností (Information Security Aspects of Business Continuity Management)

Požadavky na zajištění kontinuity činnosti informačního systému Swiss Life Select jsou určeny. Pro zajištění stanoveného rozsahu činností je zpracován a implementován havarijní plán (resp. plán obnovy) informačního systému. Pracovníci odpovědní za zajištění kontinuity činnosti organizace jsou pro svou činnost připravováni a jejich znalosti a dovednosti jsou prověřovány. Za zajištění kontinuity provozu informačního systému odpovídá vedoucí oddělení IT.

3.14 Soulad s požadavky (Compliance)

Všechny platné legislativní i smluvní požadavky na zajištění bezpečnosti informací v rámci Swiss Life Select jsou identifikovány, dokumentovány a aktivně využívány při tvorbě interních předpisů souvisejících s provozem informačního systému, sdílením a zveřejňováním dat apod.

Swiss Life Select striktně dodržuje autorský zákon a licenční ujednání softwaru, který využívá. Všichni zaměstnanci a pracovníci Swiss Life Select jsou poučeni o povinnostech vyplývajících z těchto zákonných norem.