Dodatek k přednášce Anatomie InSec
Katalog opatření, ISO/IEC 27002

PV 017 ◇ Bezpečnost IT

Jan Staudek
http://www.fi.muni.cz/usr/staudek/vyuka/

Verze : podzim 2019

ISO/IEC 27002:2013

- Information Security Management
  - ✓ *Information technology – Security techniques – Code of practice for information security management*
  - ✓ Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení informační bezpečnosti
- Struktura standardu
  - ✓ Standard obsahuje celkem 11 základních oddílů, které jsou dále rozděleny do 39 kategorií bezpečnosti
  - ✓ V každé kategorii bezpečnosti se specifikuje alespoň jedno opatření
  - ✓ Mimo to jsou ve standardu uvedeny základní informace o procesech hodnocení a zvládání rizik.
  - ✓ Oddíly jsou číslované pořadím kapitol standardu obsahujících jejich popis (5 – 15)

ISO/IEC 27002:2013, Oddíly kategorií bezpečnosti

Každý z oddílů obsahuje jednu nebo více kategorií bezpečnosti

5) Bezpečnostní politika
6) Organizace bezpečnosti – interní organizace, externí subjekty
7) Klasifikace a řízení aktiv – odpovědnosti za aktiva, klasifikace
8) Bezpečnost lidských zdrojů – přijetí do, průběh, ukončení vztahu
9) Fyzická bezpečnost a bezpečnost prostředí
10) Řízení komunikací a řízení provozu – vybraný ilustrační příklad
11) Řízení přístupu – vybraný ilustrační příklad
12) Nákup, vývoj a údržba informačního systému
13) Zvládání bezpečnostních incidentů
14) Řízení kontinuity činností organizace
15) Soulad s požadavky – práva, politik, smluv, . . . , audit

ISO/IEC 27002:2013, Popis kategorií bezpečnosti

- Popis každé z kategorií bezpečnosti obsahuje:
  - ✓ cíl opatření, určující čeho má být dosaženo;
  - ✓ popis jednoho nebo více opatření, která lze použít k dosažení stanoveného cíle opatření.
- Popis opatření je strukturován následovně:
  - ✓ Opatření –

    Přesná formulace konkrétního opatření, které vede k naplnění cíle opatření.
  - ✓ Doporučení k realizaci –

    Podrobnější informace a doporučení na podporu implementace vybraných opatření, která vedou k dosažení cíle opatření.
  - ✓ Další informace –

    Další informace, které může být potřebné vzít do úvahy, otázky legislativy, odkazy na další relevantní normy a předpisy, . . .

10. Řízení komunikací a řízení provozu

Kategorie opatření spadající do oddílu 10:

- 10.1 Operational procedures and responsibilities
  Cíl: *To ensure the correct and secure operation of information processing facilities.*
- 10.2 Third party service delivery management
  Cíl: *To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.*
- 10.3 System planning and acceptance
  Cíl: *To minimize the risk of systems failures.*
- 10.4 Protection against malicious and mobile code
  Cíl: *To protect the integrity of software and information.*

10. Řízení komunikací a řízení provozu

- 10.5 Back-up
  Cíl: *To maintain the integrity and availability of information and information processing facilities.*
- 10.6 Network security management
  Cíl: *To ensure the protection of information in networks and the protection of the supporting infrastructure.*
- 10.7 Media handling
  Cíl: *To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.*
- 10.8 Exchange of information
  Cíl: *To maintain the security of information and software exchanged within an organization and with any external entity.*

10. Řízení komunikací a řízení provozu

- 10.9 Electronic commerce services
  Cíl: *To ensure the security of electronic commerce services, and their secure use.*
- 10.10 Monitoring
  Cíl: *To detect unauthorized information processing activities.*

10.1. Provozní procedury a odpovědnosti

- Cíl – *To ensure the correct and secure operation of information processing facilities.*
- procedura ≡ pracovní postup
- Relevantní skupiny opatření v kategorii 10.1 v oddílu 10
  - ✓ Dokumentace provozních procedur
  - ✓ Změnové řízení
  - ✓ Oddělení odpovědností
  - ✓ Oddělení vývoje, testů a provozů

10.1. Dokumentace provozních procedur

- Cíl – *Operating procedures shall be documented, maintained, and made available to all users who need them*
- Provozní procedury musí vyhovovat požadavkům systému správy dokumentů organizace (principy viz ISO 9000)
  - ✓ nutné je schválení relevantním vedením organizace
- Zveřejnění provozních procedur
  - ✓ pro zaměstnance – v intranetu
  - ✓ pro partnerské třetí strany – v extranetu
  - ✓ požadavky: snadná údržba, pohotová aktualizace

10.1. Dokumentace provozních procedur

- Nezbytné provozní procedury pro ISMS identifikuje bezpečnostní politika
  - ✓ základ skladby provozních procedur tvoří ty procedury, které implementují politiku informační bezpečnosti
  - ✓ základ lze doplnit detailnějšími provozními procedurami vypracovanými na základě doporučení poradce pro ITSec a odpovědných provozních pracovníků pro typové provozní oblasti
  - ✓ nutné je jejich schválení relevantním vedením organizace

10.1. Oblasti pokrývané v ISMS provozními procedurami

- Zpracování informací a nakládání s informacemi
  - ✓ vč. požadavků na důvěrnost a klasifikaci informací
- Zálohování (detaily viz 10.5)
- Plánování činností, (např. zálohování)
  - ✓ vč. návazností na jiné systémy
  - ✓ vč. nejdřívějších a nejzazších možných termínů provedení (např. právě zálohování)
- Chybové řízení a řízení ve výjimečných podmínkách
  - ✓ vč. instrukcí pro omezené používání systému
  - ✓ vč. návodů pro nové (a nezkušené) zaměstnance (1. reakce na incident)
  - ✓ chybové řízení a řízení ve výjimečných podmínkách je jinak předmětem činnosti specialistů s dostatečnými zkušenostmi a dovednostmi

10.1. Oblasti pokrývané v ISMS provozními procedurami

- Kontaktování odpovídající podpůrných týmů v případě neočekávaných provozních nebo technických obtíží a dokumentování těchto kontaktů
- Správa speciálních výstupů (tisků)
  - ✓ vč. reakcí na selhání výstupů speciálních úloh
- Restart systému a postupy po výpadku systému
- Všechny hospodářské/udržbové činnosti
  - ✓ start a vypnutí počítače
  - ✓ údržba zařízení
  - ✓ využívání počítačového sálu, . . .
  - ✓ mají být viditelně vystavené
  - ✓ zaměstnanci mají být školení na jejich používání

10.1. Dokumentace provozních procedur, poznámky

- Zbytečně detailní procedury / řídce aplikovatelné procedury – jakoby by nebyly žádné
- Při outsourcování IT služeb musí být provozní procedury vyžádány v kontraktu

10.1. Změnové řízení

- Cíl – *Changes to information processing facilities and systems shall be controlled.*
- Řízení změn zařízení pro zpracování informací, operačních systémů a aplikačního software
- Formální, dokumentované postupy pro všechny změny těchto aktiv
- Neadekvátní úroveň změnového řízení –
  - ✓ výrazná zranitelnost
  - ✓ zdroj zbytečných nákladů
- Inovační změna musí být vyvolána adekvátními důvody, musí existovat kritéria pro rozhodování o inovaci a relevantní časové plány postupu

10.1. Změnové řízení

- procedura změnového řízení OS a aplikačních systémů – typicky 1-stránkový dokument pokrývající
  - ✓ identifikci významu změny z pohledu činností organizace (případně doplněnou o posouzení přínosu změny)
  - ✓ plán testování změny a převzetí změny uživatelem
  - ✓ posouzení možných (bezpečnostních , . . .) dopadů, vč. dopadů na jiný aplikační či provozní software a hardware
  - ✓ formální odsouhlasení změny
  - ✓ sdělení o změně všem relevantním osobám
  - ✓ postup pro zrušení změny a návrat do původního stavu
- Každá změna v síti by měla vyvolat přehodnocení hlavních rizik pro bezpečnost informací
  - ✓ a případně následné změny v prohlášení o aplikovatelnosti
- Musí se opravit všechny dokumenty závislé na měněném jevu

10.1. Oddělení povinností (oblastí odpovědnosti)

- Cíl – *Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.*
- Oddělení řídicích a výkonných povinností snižuje možnosti provedení neoprávněných úprav / zneužití informací / služeb.
  - ✓ V malých organizacích obtížně dosažitelné
  - ✓ vždy je nutné implementovat separaci v co možná největším rozsahu
  - ✓ Oddělení řízení, monitoringu a auditu je neobejitelné, audit vždy musí být nezávislý

10.1. Oddělení povinností (oblastí odpovědnosti)

- Cílem je oddělení iniciace události od povolení jejího výskytu
- prevence spáchání podvodu bez možnosti detekce v oblasti s jedinou odpovědností, tj. oddělení činností, které –
  - ✓ pro spáchání podvodu vyžadují uzavření tajné dohody (např. vystavení objednávky x potvrzení získání zboží)
  - ✓ pracují s aktivy, které posouzení rizik označilo jako podvodně manipulovatelné a musí být do manipulace s nimi zahrnuty alespoň dva interní zaměstnanci (snížení pravděpodobnosti konspirace s externí osobou)

10.1. Oddělení vývojových, testovací a provozních prostředí

- Cíl – *Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.*
- relevantní požadavek pro organizace s vlastním vývojovým střediskem
  - ✓ příp. s vývojem zajišťovaným outsourcingem
- Musí být dokumentovaná pravidla pro přenos software z vývojového do testovacího a z testovacího do provozního prostředí
- Jednotlivá prostředí mají být implementovaná na různých počítačích / v různých doménách

10.1. Oddělení vývojových, testovací a provozních prostředí

- Jednotlivá prostředí mají pracovat s různými daty
  - ✓ vývojové prostředí – umělá nebo scramblovaná živá data
  - ✓ testovací prostředí – vzorek živých dat za podmínek shodných s provozním prostředím
  - ✓ s živými daty pouze v provozním prostředí
- Musí se používat odlišné autentizační metody v jednotlivých prostředích
- Vývoj nesmí mít nikdy přístup do provozního prostředí

10.2. Řízení dodávek služeb třetích stran

- Třetí strana – jiná entita než entita přímo zahrnutá do transakcí, činností, . . . , organizace
  - ✓ Firma x *zákazníci* x třetí strana dodávající služby firmě
- Cíl – *To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.*
- Relevantní oblasti opatření
  - ✓ Dodávky služeb
  - ✓ Sledování a přezkoumávání poskytovaných dodávek služeb
  - ✓ Změnové řízení ve službách třetích stran

10.2. Dodávky služeb

- Cíl – *It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.*
- Smlouva o dodávkách s třetí stranou musí identifikovat všechna bezpečnostní opatření, definice všech služeb a formy jejich poskytování
- Outsourcing může požadovat zřízení řídicího týmu a mechanismů pro sledování výkonnosti
- Musí se pečlivě a detailně plánovat a dokumentovat předání dat třetí straně
  - ✓ vč. posouzení rizik ještě před uzavřením kontraktu

10.2. Dodávky služeb

- Smlouva by měla obsahovat doložku o možnosti požadovat navýšení síly bezpečnostních opatření
- Vždy je nutno věnovat zvláštní pozornost problémům typu
  - ✓ citlivé nebo kritické aplikace, které by mohly být lépe řešeny in-house
  - ✓ souhlas vlastníků a dodavatelů softwaru s outsourcingem procesu
  - ✓ dopady na plány zachování činnosti
  - ✓ bezpečnostní standardy, které budou závazné pro třetí strany, a jak se má soulad s nimi měřit
  - ✓ které činnosti a individuální odpovědnosti je třeba sledovat
  - ✓ zvládání bezpečnostních incidentů a zabudování smluvních procedur do politik organizace
- Důraz na smluvní závazky třetí strany v oblasti bezpečnosti
  - ✓ řízení přístupu, správa bezpečnosti podle dohodnutých standardů, . . .
- Důkladná dokumentace
  - ✓ agendy, zápisy z porad, dodatečné dohody, . . .

10.2. Sledování a přezkoumávání poskytovaných dodávek služeb

- Cíl – *The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.*
- Za dodávky služeb musí být někdo (role/oddělení) odpovědný
- Mezi klíčové odpovědnosti patří
  - ✓ sledování výkonu – zajišťování, aby se skutečně dosahovala smluvní úrovně služeb, identifikace nedostatků, a dohadování jak by nedostatky měly být opraveny.
  - ✓ přezkoumávání všech záznamů o bezpečnostních incidentech (včetně auditních zpráv), provozních problémech, poruchách, závadách a o čemkoliv jiném, co může generovat riziko pro organizaci a zajištění, aby byla přijata příslušná nápravná opatření.

    To může vést k eskalaci smluvních vztahů doplněním smluvních ustanovení o možném navýšení plnění a manažerský tým odpovědný za smlouvu by měl mít dovednosti a zkušenosti pro řízení eskalace .

10.2. Sledování a přezkoumávání poskytovaných dodávek služeb

- Žádný prostor pro nejasnosti – vše musí být dokumentované
- Musí ex. možnost přezkoumávat u třetí strany procesy změnového řízení, záznamenávání incidentů a reakcí na ně, identifikace zranitelností a uplatňování opatření
- Odpovědnost za zpracování dat má objednávající strana, odpovědnost nelze smlouvou převézt na třetí stranu
  - ✓ má-li organizace vyhovět datově orientované legislativě, musí být adekvátní procesy a systémy i u třetí strany

10.2. Změnové řízení ve službách třetích stran

- Cíl – *Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.*
- Správa změnového řízení zajišťovaného u třetí strany musí být řádně zakotveno ve smlouvě o outsourcingu
  - ✓ jedná se o mezi-organizační procesy
  - ✓ musejí být odsouhlaseny oboustranně
- Jedná se o všechny změny mající dopad na inf. bezpečnost
  - ✓ musí se provést posouzení rizik následované identifikací a implementací relevantních opatření
- Změnu může iniciovat i třetí strana (podle pravidel ve smlouvě)

10.3. Plánování a přejímání systémů

- Cíl – *To minimize the risk of systems failures.*
- Relevantní oblasti opatření
  - ✓ Správa kapacit
  - ✓ Přejímání systémů

10.3. Správa kapacit

- Cíl – *The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.*
- Organizace má sledovat požadavky na kapacity a prognózovat jejich vývoj
  - ✓ souborové / doménové servery, tiskárny, komunikační spoje, . . .
  - ✓ zvýšení aktivit si vyžádá zvětšení týmu, bude potřeba více osobních počítačů, . . .
  - ✓ nárůst webových aktivit při e-komerci
- Nedostatečné kapacity jsou zdroje bezpečnostních incidentů typu DoS (*Denial of Services*)

10.3. Přejímání systémů

- Cíl – *Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.*
- Organizace má stanovit přejímací kritéria pro nové systémy, vylepšení systémů, pro jejich nové verze
  - ✓ při přejímání musí proběhnout relevantní testy
- Přejímací kritéria musí být stručná, jasná, (smluvně) odsouhlasená a dokumentovaná

10.3. Přejímání systémů

- Přejímání nové verze systému vyžaduje provést kontroly splnění požadavků daných činností organizace na:
  - ✓ na výkony počítačů a kapacity
  - ✓ revize / vytvoření nových programů pro obnovu po poruchách a restart
  - ✓ přepracování a otestování rutinních provozních procedur
  - ✓ implementaci nových bezpečnostních opatření po znovu provedeném posouzení rizik
  - ✓ vypracování nových manuálů a dokumentovaných provozních procedur
  - ✓ inovaci plánu zachování kontinuity činnosti organizace
  - ✓ podání důkazů, že nové systému nemají nepříznivý vliv na běžící existující systémy
  - ✓ podání důkazů posouzením rizik jaký má dopad nový systém na celkovou bezpečnost organizace
  - ✓ zaškolení uživatelů na nový systém a posouzení dopadu na uplatňované pracovní praktiky

10.3. Přejímání systémů

- Má se provozovat nový systém po jistou dobu souběžně s původním systémem ?
- Zvláštní pozornost je potřeba věnovat přejímacím kritériím pro nové komunikační systémy
- Posouzení rizik může vyžádat provedení testů, verifikací a certifikací nezávislou třetí stranou

10.4. Ochrana proti škodlivým a mobilním programům

- Cíl – *To protect the integrity of software and information.*
- Relevantní oblasti opatření
  - ✓ Opatření proti škodlivým programům

    'Malware' is a term that denotes software designed for some malicious purpose.
    programy, které na počítači běží bez vědomí uživatele a nějakým způsobem jej poškozují, nebo zhoršují jeho funkci – viry, červi, Trojští koně, . . . , spyware
  - ✓ Opatření proti mobilním programům

    'program that can execute on remote locations with any modification in the code. [It] can travel and execute from one machine to another on a network during its lifetime' – software transferred between systems, e.g. transferred across a network or via a USB flash drive, and executed on a local system without explicit installation or execution by the recipient

    ActiveX, Java, JavaScript, VBScript, MS Word macros, PostScript, . . .

10.4. Opatření proti škodlivým programům

- Cíl – *Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.*
  - ✓ ISMS má obsahovat politiku a procedury požadující vyhovění softwarovým licencím a zakazující používat neutorizovaný software
  - ✓ ISMS má obsahovat politiku a procedury chránící organizaci proti importu škodlivého software – zákaz přímého přístupu uživateli na externí disky, CD-ROM, USB paměti apod. Data z nich může zavádět pouze IT tým po kontrole.
  - ✓ V síti organizace má být instalovaný aktualizovaný ,,anti-malware software''
  - ✓ Bez prodlení instalovat opravy (záplaty) zveřejněné výrobcem licencovaného software a o všech instalací záplat vést auditní záznamy (kdy, kdo, co instaloval)
  - ✓ Pravidelně přezkoumávat software a data na všech počítačích organizace a odhalovat a odstraňovat neautorizované programy / data

10.4. Opatření proti škodlivým programům

- ✓ Všechny soubory z externích zdrojů kontrolovat na výskyt škodlivého software
- ✓ Všechny přílohy e-mailů kontrolovat na firewallu na výskyt škodlivého software
- ✓ Zaměstnance proškolovat v rozpoznávání potenciálně napadených e-mailů škodlivým software
- ✓ Ustanovení odpovědnosti za běh ochran proti škodlivému software, detekce incidentů a odtraňování důsledků činnosti škodlivého software se má řešit dokumentovanými procedurami
- ✓ Má existovat BCP pro obnovu po útoku škodlivým software
- ✓ Bezpečnostní manažeři mají mít přístup ke vhodným a důvěryhodným zdrojům aktuálních informací o škodlivém software
- ✓ Mají být instalovány opatření proti spyware
- ✓ Zaměstnanci mají být školení jak záchazet s webovskými uzly napadnutými škodlivým software

10.4. Opatření proti mobilním programům

- □ Cíl – *Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to clearly defined security policy, and unauthorized mobile code shall be prevented from executing.*
  - ✓ triviální řešení – politikou zakázat instalaci a na firewallu blokovat software obsahující mobilní kód
  - ✓ blokování lze omezit na vybrané podezřelé uzly

10.5. Zálohování

- □ Cíl: *To maintain the integrity and availability of information and information processing facilities.*
- □ Relevantní oblasti opatření
  - ✓ Zálohování informací

10.5.Zálohování informací

- □ Cíl – *Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.*
  - ✓ Ideál – všechny informace organizace uchovávat na serverech organizace a servery pravidelně (automaticky) zálohovat
  - ✓ Povinnost zálohovat data z přenosných zařízeních na serverech organizace má být součástí iniciálního bezpečnostního školení zaměstnance
  - ✓ politika zálohování musí pokrývat všechna potenciální místa obsahující citlivá data organizace
  - ✓ zálohovat je potřeba data originálně uchovávaná nejen v elektronické, ale i v papírové formě
  - ✓ musí se určit metody a frekvence zálohování

10.5.Zálohování informací

- ✓ zálohované informace společně s úplnými a přesnými záznamy o tom co je zálohováno a dokumentace procedur obnovy se má uchovávat ve vzdálené lokalitě
- ✓ zálohání lze řešit kontraktem s třetí stranou
- ✓ zálohovací cyklus má implementovat 3-generační postup aplikovaný na měsíční, týdenní a denní zálohy:
  - syn: každý den v týdnu samostatně, přepis každý týden
  - otec: každý týden v měsící, přepis každý měsíc
  - dědeček: každý měsíc v roce, přepis každý rok
- ✓ na zálohy se musí aplikovat stejná bezpečnostní opatření jako na originální data, případně je navíc utajovat šifrováním
- ✓ zálohovací média je potřeba pravidelně testovat na zpracovatelnost
- ✓ pravidelně se mají testovat všechny obnovovací procedury dokumentované v ISMS a výsledky testů se mají uchovávat v dokumentaci BCP

10.5.Zálohování informací

- ✓ zálohování má být předmětem pravidelného přezkoumávání managementem
- ✓ Kritické aplikace mají být provozované na serverech implementovaných na technologii RAID (ideálně RAID 5)
- ✓ má být stanovena doba uchovávání záloh podle omezení daných požadavkem vyhovění legislativě, smluvním závazků a byznys modelu

10.6. Síťová bezpečnost

- □ Cíl: *To ensure the protection of information in networks and the protection of the supporting infrastructure.*
- □ Relevantní oblasti opatření
  - ✓ Síťová opatření
    – *Internet acceptable use policy*, AUP
  - ✓ Bezpečnost síťových služeb

10.6. Síťová opatření

- □ Cíl – *Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.*
  - ✓ odpovědnost za provoz sítě řešit odděleně od administrace počítačů – viz Oddělení/Oddělení povinností
  - ✓ jednoznačně definovat odpovědnosti a procedury správy vzdálených zařízení vč. oblastí vzdálených uživatelů
  - ✓ speciální opatření se musí přijato pro ochranu dat přenášených bezdrátovými a veřejnými sítěmi
  - ✓ v celé síti musí být musí být konzistentně aplikovaná opatření definovaní v ISMS
  - ✓ musí být dokumentovaná architektura celé sítě vč. detailů konfiguračních nastavení a specifikace všech softwarových a hardwarových komponent

10.6. Internet acceptable use policy, AUP

- Musí být v písemné formě
- Musí být srozumitelně sdělena všem zaměstnancům
- Nastavuje povolené používání jak Internetu, tak i e-mailu, má kombinovat prohlášení o používání Internetu a využívání e-mailu
- Specifilkuje, které používání Internetu je zakázano – např. stahování nepřístojných dokumentů, pornografie a nezákonných materiálů
- Sděluje, co se monitoruje
- Definuje přijatelné on-line chování

10.6. Internet acceptable use policy, AUP

- Udává zákázané on-line oblasti – např. pornografické / rasistické servery
- Nastavuje pravidla zachování soukromí ve vztahu k ostatním uživatelům při respektování práva zaměstnavatele sledovat aktivity zaměstnanců
- Sděluje co jsou pravděpodobné disciplinární důsledky porušení pravidel AUP

10.6. Internet acceptable use policy, AUP

- Úvod AUP tvoří souhrnné prohlášení
  - ✓ Mělo by začít s připomenutím hrozeb Internetu a říci, že organizace nebude odpovědná za jakékoli stažené či prohlížené materiály. Dále se má sdělit, že používání Internetu musí být v souladu se standardy plnění činností organizace a je součástí pracovních povinností zaměstnance.
  - ✓ Jakékoli porušení AUP může vést k disciplinárnímu řízení a příp. i k ukončení zaměstnání.
  - ✓ Nezákonné činnosti mohou být oznámeny příslušným orgánům.

10.6. Internet acceptable use policy, AUP

- Generické body obsahu AUP
  - ✓ Uživatelské ID organizace, weby a e-mailové účty lze používat pouze pro komunikaci schválenou organizací
  - ✓ Použití internetu/intranetu/e-mailu/konverzačních systémů může být předmětem sledování a uživatelé mohou být při používání těchto zdrojů omezováni.
  - ✓ Distribuce informací prostřednictvím Internetu (včetně e-mailu a jiných počítači podporovaných systémů) může být organizací kontrolována a organizace si rezervuje právo stanovit vhodnosti informace.
  - ✓ Používání počítačových prostředků organizace podléhá právu a zneužití bude adekvátně potrestáno.
  - ✓ Uživatelé nesmí navštěvovat internetové stránky, které obsahují vulgární, nenávistné nebo nežádoucí materiály a nesmí obcházet opatření omezující prohlížení a na Internet nesmí učinit nebo vystavit neslušné poznámky, návrhy nebo materiály.

10.6. Internet acceptable use policy, AUP

- ✓ Uživatelé nesmí rozesílat e-maily, které nesouvisí s činností organizace nebo pro svůj osobní prospěch, nesmí odesílat nebo přijímat jakýkoli obscénní či hanlivý materiál nebo materiál určený k obtěžování nebo k zastrašování jiné osoby a nesmí předkládat své osobní názory jako názory organizace.
- ✓ Uživatelé nesmí ukládat, stahovat nebo jinak přenášet komerční software a/nebo autorsky chráněný materiál, patřící organizaci nebo kterékoliv jiné třetí straně
- ✓ Uživatel nesmí ani odhalit ani zveřejnit důvěrné informace (uvede se klasifikační úroveň) a nesmí odeslat důvěrné e-maiy bez zašifrování na úrovni vyžadované politikou ISMS.
- ✓ Uživatelé se nesmí pokoušet obcházet politiku prevence uplatnění škodlivého software a musí zachovávat všechny odpovídající politiky organizace,

10.6. Internet acceptable use policy, AUP

- ✓ Uživatel záměrně nezasahuje do normální činnosti sítě a ani nečiní žádné kroky, které by ostatním bránily ve využívání sítě a nesmí bez explicitního povolení zkoumat, měnit nebo používat soubory jiných osob nebo jakékoli jiné informační aktivum
- ✓ Uživatelé nesmí vykonávat jakékoliv jiné nevhodné aktivity, které v jistých časových intervalech označuje organizace, a nesmí mrhat časem neo i jinými zdroji na činnosti nesouvisející s činnostmi organizace. Myslí se tím stahování ze serverů sociálních sítí, servery, objemy dat náročné na šířku pásma, jako jsou například videa a hudební soubory MP3, sdílení digitálních fotografií atd.

10.6. Bezpečnost síťových služeb

- □ Cíl – *Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.*
- □ Síťové služby může poskytovat organizace interně nebo outsourcingem
- □ Příklady –
  application service providers (ASP),
  Internet service providers (ISPs),
  serverové farmy,
  služby poskytující dedikované informace, . . .

10.6. Bezpečnost síťových služeb

- □ Je nutné identifikovat a dokumentovat bezpečnostní charakteristiky síťových služeb
  - ✓ bezpečnostní technologie (šifrování, autentizace, typ síťového spojení, . . .)
  - ✓ technické parametry pro bezpečné spojení s poskytovatelem služby
  - ✓ procedury pro omezení přístupu ke službám, existují-li
  - ✓ opatření vztahující se k údajům uchopvávaným v systému (např. osobní data)

10.7. Správa médií

- Cíl: *To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.*
- Relevantní oblasti opatření
  - ✓ Správa výměnných médií
  - ✓ Skladováni médií
  - ✓ Procedury pro manipulací s informacemi
  - ✓ Bezpečnost systémové dokumentace

10.7. Správa výměnných médií

- Cíl – *There shall be procedures in place for the management of removable media.*
- pásky, disky, kazety, tištěné zprávy
- ochrana před zničením, krádeží, neautorizovaným přístupem
  - ✓ manipulaci s USB pamětmi apod. musí definovat bezpečnostní politika
  - ✓ médium odstraňované z organizace musí být vymazáno, plně, ne pouze co je vidět v adresáři
  - ✓ vynášení média mimo budovu má být explicitně povolováno a dokumentováno, pravidelné vynášení (zálohy) má řídit procedura
  - ✓ skladování médií musí vyhovovat pravidlům stanovených výrobcem
  - ✓ je nutno respektovat dobu životnosti stanovenou výrobcem

10.7. Skladováni médií

- Cíl – *Media shall be disposed of securely and safely when no longer required, using formal procedures.*
- ISMS musí obsahovat procedury zajišťující bezpečné skladování médií obsahujících
  - ✓ listinné dokumenty
  - ✓ hlasové a videozáznamy
  - ✓ kopíráky
  - ✓ výstupní zprávy
  - ✓ tiskárenské pásky
  - ✓ USB paměti
  - ✓ CD ROM
  - ✓ listingy programů, testovací data, dokumentace systému, . . .
- nutné jsou procedury skartace a likvidace

10.7. Procedury pro manipulací s informacemi

- Cíl – *Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.*
- procedury musí pokrývat
  - ✓ převoz médií
  - ✓ řízení přístupu
  - ✓ určení autorizovaného příjemce dat na bázi klasifikace dat
  - ✓ zajištění kompletnosti vstupních dat, zpracování, validace výstupů
  - ✓ zacházení s médiu podle specifikace výrobcem
  - ✓ distribuci dat vyhovující klasifikačním schématům
  - ✓ pravidelné přezkoumávávní distribučních a autorizačních seznamů zda obsahují aktuální cíle

10.7. Bezpečnost systémové dokumentace

- Cíl – *System documentation shall be protected against unauthorized access.*
  - ✓ ochrana před neautorizovaným přístupem
  - ✓ nejde o veřejně dostupné manuály, ...
  - ✓ jde o vnitřní dokumentaci organizace popisující systémy, procesy, struktury dat, autorizační procesy, ...

10.8. Výměna informací

- Cíl: *To maintain the security of information and software exchanged within an organization and with any external entity.*
- Relevantní oblasti opatření
  - ✓ Politiky a procedury při výměně informací
  - ✓ Dohody o výměně informací a programů
  - ✓ Fyzická média při přepravě
  - ✓ Elektronické zasílání zpráv
  - ✓ Aplikační informační systémy organizace
- E-mail téměř zcela nahradil dálnopis a zjevně brzo nahradí fax a tradiční poštu.
  - ✓ E-mail se od běžné pošty odlišuje – má vysokou rychlost, jinou strukturu zpráv, nízkou formálnost, vykazuje možnost chybného doručení, kopírování, snadného zachycení a možnost přenosu příloh.

10.8. Politiky a procedury při výměně informací

- Cíl – *Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.*
- Výměna informací formami
  - ✓ komunikační linky, e-mail, hlas, fax, video, ...
- Opatření musí zajišťovat ochranu proti neautorizovanému
  - ✓ zachycování, kopírování, modifikování, přesměrovávání, rušení, ... informací
- Použité mechanismy
  - ✓ Vodoznaky, šifrování, ... pro zajištění důvěrnosti, integrity, autenticity, ...
- Nutnost respektovat klasifikační schéma, legislativní omezení, ...

10.8. Politiky a procedury při výměně informací

- Musí se přijmout politika ochrany proti škodlivému software a musí se implementovat relevantní opatření
- Citlivé dokumenty se nesmí tisknout / ponechávat ve veřejně dostupných tiskárnách / faxech, musí být zasílané na dedikovaná zařízení
- Je potřeba srozumitelně identifikovat hrozbu komunikace v bezdrátovém prostředí a do prohlášení o aplikovatelnosti dát adekvátní politiku a opatření
- Použití telefonů a mobilů z míst, která nejsou bezpečná, nesmí vyzradit důvěrnou informaci (veřejné prostory, kanceláře s tenkými stěnami, areál konkurenta, přeplněný vlak ...)

10.8. Politiky a procedury při výměně informací

- Nepoužívat pro důvěrnou výměnu informací zařízení, která lze snadno kompromitovat (telefon v areálu konkurenta) nebo jsou automaticky nahrávaná (banky, . . .)
- Důvěrnou informaci nesdělovat do hlasové schránky nebo pomocí SMS
- E-mail lze snadno chybně nasměrovat, před odesláním se musí pečlivě ověřit všichni adresáti
- Důvěrné informace se nesmí posílat faxem

10.8. Dohody o výměně informací a programů

- Cíl – *Agreements shall be established for the exchange of information and software betweenthe organization and external parties.*
- Smlouva musí specifikovat bezpečnostní podmínky výměn dané schématem klasifikace informací
- Zavedení výměn může si vyžádat provedení ohodnocení rizik
- Musí se identifikovat na obou stranách kdo je odpovědný za řízení, oznamování, zahajování a přijímání výměn
- Musí se definovat procedury sdělující druhé straně odeslání / přijetí citlivé informace a opatření zajišťující sledovatelnost a nepopiratelnost
- Musí se určit technické standardy pro balení a přenos informací

10.8. Dohody o výměně informací a programů

- Musí se určit kurýrní identifikační procedury
- Musí se určit odpovědnosti a ručení za ztrátu informací nebo bezpečnostní incidenty
- Musí se dohodnout systém označování, který zajistí, že se bezprostředně zjistí a poskytnou odpovídající ochrany. Měl by být shodný se systémem používaným v organizaci interně.
- Musí určit odpovědnost za vlastnictví informací a software, ochrany dat, autorská práva apod.
- Mají se určit technické standardy pro zápis / čtení informací
- Musí se definovat specifická opatření (např. kryptografická), která mohou být potřebná pro konkrétní citlivé informace

10.8. Fyzická média při přepravě

- Cíl – *Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.*
- Nejčastěji se přepravují CD-ROMy a pásky
- Pošta a občasná kurýrní služba nejsou bezpečné přepravní systémy
- Je nutné přijmout opatření typu
  - ✓ šifrování, pokud médium obsahuje citlivé / osobní data
  - ✓ udržovat seznam spolehlivých, důvěryhodných kurýrních služeb, případně používat smluvně vázanou kurýrní službu jako službu poskytovanou třetí stranou
  - ✓ Balení hardware musí respektovat požadavky jeho výrobce
  - ✓ Případně používat fyzická opatření (zamykatelné kontejnery, . . .)

10.8. Elektronické zasílání zpráv

- Cíl – *Information involved in electronic messaging shall be appropriately protected.*
- Politika bezpečného používání e-mailu
- Generická rizika e-mailu
  - ✓ zranitelnost neautorizovaným přístupem, neautorizovanou modifikací a útoky typu DoS
  - ✓ zranitelnost nesprávným adresováním, chybným směrováním a nespolehlivostí Internetu
  - ✓ legislativní problémy – nejsou dostupné důkazy původu, odeslání a příjmu
  - ✓ neovladatelnost vzdáleného uživatele

10.8. Elektronické zasílání zpráv

- Politika bezpečného používání e-mailu by měla zajistit
  - ✓ Odpovědnost zaměstnance nekomprmitovat organizaci zakazující použití e-mailů společnosti pro zasílání hanlivých mailů nebo pro obtěžování, pro neoprávněné nákupy nebo publikování názorů na dodavatele, partnery či zákazníky z organizace.
  - ✓ E-mail by se neměl používat pro komunikaci citlivé informace s jistou klasifikací
  - ✓ Přílohy e-mailů by měl být vhodně chráněny, (případně) pomocí kryptografických kontrol nějakého typu
  - ✓ Jak reagovat na viry a podvod zavirovanou zprávou
  - ✓ Velikost schránky s příchozí poštou musí být zajištěna procedurou
  - ✓ Bez konkrétního předchozího povolení nelze používat e-mail pro nákup jménem organizace. Pokud lze, pak jen v souladu s aktuální politikou organizace pro nákupu.
  - ✓ Firemní e-mailová adresa nesmí být použita pro osobní nákupy nebo jiné osobní transakce.

10.8. Aplikační informační systémy organizace

- Cíl – *Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.*
- Současné distribuované systémy dramaticky zvyšují elektronickou komunikaci mezi zaměstnanci a možnost sdílení informací
  - ✓ F2F komunikace je vrozeně bezpečnější
- Doporučená opatření
  - ✓ Jasně definovaná politika sdílení informací respektující schéma
  - ✓ Jestliže nelze zajistit adekvátní ochranu proti přístupu zvenčí organizace, pak chráněnou informaci nelze publikovat na vnitroorganizačních nástěnkách
  - ✓ Opatření zajišťující bezpečnou komunikaci via rizikový Internetí

10.8. Aplikační informační systémy organizace

- ✓ Osobní kalendáře akcí zveřejňovat pouze spolupracovníkům na projektu, . . .
- ✓ Pro každý aplikační informační systém by měla být stanovena požadovaná výše záruky za bezpečnost a její dosažení prokázat evaluací
- ✓ ISMS požaduje identifikovat kategorie zaměstnanců a smluvních partnerů s povoleným přístupem k systémů a lokality, odkud lze systémy zpřístupňovat
- ✓ ISMS požaduje určit přístupová práva k aplikačním systémům jednotlivcům, na základě jejich rolí v organizačním schématu
- ✓ E-mail musí rozlišovat mezi interními a externími adresami, aby uživatelé mohli omezit cirkulaci informací
- ✓ Musí být zavedena politka zálohování a obnov
- ✓ Musí být zavedena politika činnosti organizace v nouzovém režimu

10.9. Elektronické obchodování

- Cíl: *To ensure the security of electronic commerce services, and their secure use.*
- Relevantní oblasti opatření
  - ✓ Elektronické obchodování
  - ✓ On-line transakce
  - ✓ Veřejně dostupné informace

10.9. Elektronické obchodování

- Cíl – *Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.*
- Hlavní problém elektronického obchodování – nepopiratelnost
  - ✓ nepopiratelnost původu – jistota pro přijímací stranu, že odesílatel není podvodník
  - ✓ nepopiratelnost odeslání – důkaz, že v jistém čase věc byla odeslána
  - ✓ nepopiratelnost přijetí – důkaz, že přijímací strana skutečně zzískala odeslanou věc, druhosledově kdy a kde
- Ochrana Web serverů před útoky
- Ochrana komunikací – SSL, IPSec, PKIX, S/MIME, . . .

10.9. Elektronické obchodování

- Opatření musí zajistit, že obchodování přes veřejné sítě je chráněné před podvody, smluvními rozepřemi, neautorizovaným zpřístupněním a modifikací důvěrných dat
- Mezi stranami se musí dohodnout (příklad pro B2B)
  - ✓ Autentizace – posílení důvěry mezi zákazníkem a obchodníkem
  - ✓ Autorizace – strany musí vědět že smluvní vztahy byly domluveny s autorizovanou rolí
  - ✓ Prodejní procesy – s nepopiratelností, důvěrností, integritou, důkazy odeslání a příjmu dokumentů
  - ✓ Jak důvěrné jsou domluvy o slevách
  - ✓ Jaká je důvěrnost chráněných transakčních detailů (platba, detaily dodávky, . . .)

10.9. Elektronické obchodování

- ✓ Co se musí ověřovat na platebních informacích
- ✓ Nejbezpečnější metodu plateb a jak se bude řešit podvod s padělanou platební kartou
- ✓ Jak se zabrání duplikacím a ztrátám transakcí
- ✓ Kdo nese odpovědnost za škody podvodnými transakcemi a jak se řeší pojištění

10.9. On-line transakce

- Cíl – *Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.*
- Vhodná opatření
  - ✓ Elektronické podpisování – vesměs pro B2B, často nepraktické pro C2B
  - ✓ Zajištění důvěrnosti transakcí (pomocí SSL), zajištění ochrany osobních dat
  - ✓ Plné šifrování komunikací
  - ✓ Bezpečnost musí být řešena v koncových systémech
  - ✓ Musí se respektovat legislativní omezení

10.9. Veřejně dostupné informace

- Cíl – *The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.*
- Typy opatření
  - ✓ Informace publikovaná na webu má být odsouhlasená předem
  - ✓ Informace získávaná z veřejných webů od lidí smí být shromažďována v souladu s omezeními danými legislativou
  - ✓ Webovské aplikace musí filtrovat uživateli dodávaná data (viz OWASP)
  - ✓ Citlivá data musí být při získávání a ukládání adekvátně chráněna (platební informace z karet apod. – SSL, 3D-Secure, . . .)

10.10. Sledování, monitorování

- Cíl: *To detect unauthorized information processing activities.*
- Relevantní oblasti opatření
  - ✓ Pořizování auditních záznamů
  - ✓ Monitorování používání systému
  - ✓ Ochrana auditních záznamů
  - ✓ Administrátorský a operátorský deník
  - ✓ Deníky selhání
  - ✓ Synchronizace času
- Detekce odchylek učinků přijatých opatření
  - ✓ odchylek od politiky řízení přístupu
  - ✓ detekce opakovaného zneužívání, . . .
- Získávání důkazů pro následné řešení bezpečnostních incidentů a podkladů pro kontrolu efektivnosti přijatých opatření

10.10. Pořizování auditních záznamů

- Cíl – *Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed periodto assist in future investigations and access control monitoring.*
- Záznamy o výjimkách událostech souvisejících s informační bezpečností
- Musí se uchovávat po stanovenou dobu
  - ✓ zdroj informací o tom co funguje špatně
- Za vedení odpovídá CISO, co se sleduje obvykle stanovuje řídicí výbor ITSec
- Sbírat se musí nutné informace, ne ,,všechny''informace

10.10. Pořizování auditních záznamů

- Typicky sledované informace, příklady
  - ✓ ID uživatele, doba přihlášení / odhlášení
  - ✓ úspěšné a neúspěšné přístupy uživatelů k aktivům
  - ✓ změny v konfiguraci systému
  - ✓ použití aplikací
  - ✓ aktivace / deaktivace ochran (anti-vir)
  - ✓ veškerá narušení pravidel bezopečnostní politiky
  - ✓ upozornění z firewalů a systémů detekce průniků, . . .
- Auditní deník musí být silně přístupově chráněný, slouží mj. pro odhalení neautorizovaných přístupů
  - ✓ jeho vedení by mělo zajišťovat Oddělení interního auditu
  - ✓ IT administrátoři nemají mít k deníku přístup a nesmějí mít možnost vypínat své sledování

10.10. Monitorování používání systému

- Cíl – *Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.*
- organizace musí mít zavedeny procedury pro sledování zpracování informací
- záznamy ze sledování se musí pravidelně zkoumat
  - ✓ frekvenci zkoumání určí výsledek posouzení rizik

10.10. Ochrana auditních záznamů

- Cíl – *Logging facilities and log information shall be protected against tampering and unauthorized access.*
- Je nutná striktní autorizace modifikačních přístupových práv
- Záznamy lze používat jako důkazy při soudních sporech
- Objemy zaznamenávaných informací bývají obrovské
  - ✓ je nutné stanovit politiku bezpečné archivace záznamů
  - ✓ ideální řešení – datové trezory

10.10. Administrátorský a operátorský deník

- Cíl – *System administrator and system operator activities shall be logged.*
- Příklady zaznamenávaných událostí
  - ✓ spuštění a zastavení činnosti, kdo tak učinil
  - ✓ popis akce (zahrnuté procesy, soubory, . . .)
  - ✓ chyby systému (co, kdy) a opravné akce
  - ✓ vše co souvisí se zálohováním a obnovou
  - ✓ jméno osoby učinvší záznam

10.10. Deníky selhání

- Cíl – *Faults shall be logged, analyzed, and appropriate action taken.*
- O selháních mají být vedeny záznamy, tyto mají být analyzované a závady mají být odstraňované

10.10. Synchronizace času

- Cíl – *The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.*
  - ✓ Např. zkoumání záznamů o bezpečnostních incidentech vyžaduje informaci o čase výskytů událostí
- Hodiny ve všech počítačích mají být synchronizované buďto s UCT (*Universal Coordinated Time*) nebo s lokálním standardním časem
  - ✓ dopad driftu hodin v počítačích, ...
- Mají se používat standardizované formáty vyjádření času
  - ✓ nerespektování letního času může mít negativní dopad na zkoumání auditních záznamů, ...
  - ✓ chybná interpretace času brání zkoumání událostí, přípravě důkazů, ...

11. Řízení přístupu – vybraný ilustrační příklad oddílu

- Oddíl 11. Řízení přístupu obsahuje 7 kategorií bezpečnosti
  - ✓ 11.1 Požadavky na řízení přístupu – vybraný ilustrační příklad kategorie bezpečnosti
  - ✓ 11.2 Řízení přístupu uživatelů
  - ✓ 11.3 Odpovědnosti uživatelů
  - ✓ 11.4 Řízení přístupu k síti
  - ✓ 11.5 Řízení přístupu k operačnímu systému
  - ✓ 11.6 Řízení přístupu k aplikacím a informacím
  - ✓ 11.7 Mobilní výpočetní zařízení a práce na dálku

11.1 Požadavky na řízení přístupu

- Cíl – Řídit přístup k informacím
  - ✓ Přístup k informacím, prostředkům pro zpracování informací a procesům organizace by měl být řízen na základě provozních a bezpečnostních požadavků organizace
  - ✓ Měla by být zohledněna pravidla organizace pro šíření informací a pravidla, podle nichž probíhá schvalování.
- Výčet opatření
  - ✓ 11.1.1 Politika řízení přístupu
  - ✓ Tato kategorie zavádí jediné opatření – politiku řízení přístupu

11.1.1 Politika řízení přístupu

- Opatření
  - ✓ Měla by být vytvořena, zdokumentována a v závislosti na aktuálních bezpečnostních požadavcích přezkoumávána politika řízení přístupu
- Doporučení k realizaci
  - ✓ Přístupová pravidla a oprávnění by měla být jasně stanovena pro každého uživatele nebo skupinu uživatelů v seznamu pravidel přístupu.
  - ✓ Pravidla by měla pokrývat jak logický, tak fyzický přístup, oba typy přístupů by měly být řešeny současně.
  - ✓ Uživatelům a poskytovatelům služeb by mělo být předáno jasné vyjádření o provozních požadavcích, které naplňuje řízení přístupu.

11.1.1 Politika řízení přístupu

- Doporučení k realizaci (pokrač.) –

  Politika řízení přístupu by měla brát v úvahu následující hlediska:
  - ✓ bezpečnostní požadavky jednotlivých aplikací organizace
  - ✓ identifikace všech informací ve vztahu k jednotlivým aplikacím a rizika, kterým jsou informace vystaveny
  - ✓ pravidla pro šíření informací a pravidla schvalování, tj. princip potřeby znát, bezpečnostní úrovně a klasifikaci informací
  - ✓ konzistence přístupových pravidel a klasifikace informací pro různé systémy a sítě
  - ✓ odpovídající legislativu a ostatní smluvní závazky ve vztahu k ochraně přístupu k datům nebo službám
  - ✓ standardní přístupové profily uživatelů pro běžné kategorie činností

11.1.1 Politika řízení přístupu

- ✓ řízení pravidel přístupu v distribuovaném a síťovém prostředí rozeznávajícím všechny možné typy připojení
- ✓ oddělení jednotlivých rolí pro řízení přístupu, např. vyřizování požadavků na přístup, schvalování přístupu, správa přístupů
- ✓ požadavky na formální schválení žádostí o přístup
- ✓ požadavky na pravidelné přezkoumávání přístupových práv
- ✓ podmínky a postupy pro odebrání přístupových práv

11.1.1 Politika řízení přístupu

- Další informace
  - ✓ rozlišovat mezi pravidly, která musí být v platnosti vždy, a těmi, která jsou nepovinná nebo podmíněná
  - ✓ stanovit pravidla na základě principu ,,Všechno, co není výslovně povoleno, je zakázáno“, ne na základě měkčího pravidla ,,Všechno, co není výslovně zakázáno, je povoleno“
  - ✓ zohledňovat změny ve označování informací, které jsou vyvolány automaticky prostředky pro zpracování informací, a změny, které jsou vyvolány z rozhodnutí uživatele
  - ✓ zohledňovat změny uživatelských oprávnění, které jsou vyvolány automaticky prostředky pro zpracování informací, a ty, které jsou vyvolány administrátorem
  - ✓ rozlišovat pravidla, která vyžadují schválení administrátorem nebo jinou pověřenou osobou, a ta, která toto nevyžadují.

11.1.1 Politika řízení přístupu

- ✓ Pravidla pro řízení přístupu by měla být podporována zavedením formálních postupů a jasně určených odpovědností
- ✓ Uživatelé mají znát cíle činnosti organizace, které politika přístupu dosahuje
- ✓ Opatření mohou být jak fyzického, tak i logického typu
- ✓ Uživatelé mají být školení na pravidla a politiku řízení přístupu
- ✓ Rozdílné aplikační činnosti organizace mívají rozdílné požadavky na bezpečnost – kdo má nebo nemá mít přístup k systému ukáže ohodnocení rizik
- ✓ Vhodný je princip „need-to-know"
  - Např. referentka zadávající objednávku platebnímu systému nemusí mít právo příkazce operace provedení platby
- ✓ Musí se respektovt systém klasifikace informací
  - Požadavek konzistence klasifikačních schémat a řízení přístupu a různých sítích téže organizace

11.1.1 Politika řízení přístupu

- ✓ Musí se zohledňovat relevantní legislativa
- ✓ Pro zavedené kategorie pracovních funkcí mají být definované standardizované profily uživatelských přístupů
- ✓ V distribuovaných systémech je nutné řešit přístupová práva jak při lokálním přístupu, tak i vzdáleném přístupem jednoho a téhož uživatele
- ✓ Vhodné je dodržovat princip separace odpovědností
  - V dostatečně velkých organizacích vždy oddělit role odpovědné za plnění přístupových požadavků, za jejich autorizaci a za jejich nastavení
- ✓ Pravidelně přezkoumávat opatření řídicí přístupy, přístupy je nutné průběžně monitorovat
- ✓ Rušit přístupová práva při výpovědi
- ✓ Některá pravidla politiky řízení přístupu mohou být prosazovaná trvale, jiná volitelně, příp. podmínečně nebo pouze v jistých situacích

11.1.1 Politika řízení přístupu

- ✓ Musí být stanovena přístupová práva k provedení změn v klasifikaci informaci, v pravidlech řízení přístupu, v uživatelských přístupových profilech, . . .

Skladba opatření ostatních kategorií řízení přístupu

- □ 11.2 Řízení přístupu uživatelů
  - ✓ Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.
  - ✓ Registrace uživatele
  - ✓ Řízení privilegovaného přístupu
  - ✓ Správa uživatelských hesel
  - ✓ Přezkoumání přístupových práv uživatelů
- □ 11.3 Odpovědnosti uživatelů
  - ✓ Cíl: Předcházet neoprávněnému uživatelskému přístupu, vyzrazení nebo krádeži informací a prostředků pro zpracování informací.
  - ✓ Používání hesel
  - ✓ Neobsluhovaná uživatelská zařízení
  - ✓ Zásada prázdného stolu a prázdné obrazovky monitoru

Skladba opatření ostatních kategorií řízení přístupu

- 11.4 Řízení přístupu k síti
  - ✓ Cíl: Předcházet neautorizovanému přístupu k síťovým službám.
  - ✓ Politika užívání síťových služeb
  - ✓ Autentizace uživatele pro externí připojení
  - ✓ Identifikace zařízení v sítích
  - ✓ Ochrana portů pro vzdálenou diagnostiku a konfiguraci
  - ✓ Princip oddělení v sítích
  - ✓ Řízení síťových spojení
  - ✓ Řízení směrování sítě

Skladba opatření ostatních kategorií řízení přístupu

- 11.5 Řízení přístupu k operačnímu systému
  - ✓ Cíl: Předcházet neautorizovanému přístupu k operačním systémům.
  - ✓ Bezpečné postupy přihlášení
  - ✓ Identifikace a autentizace uživatelů
  - ✓ Systém správy hesel
  - ✓ Použití systémových nástrojů
  - ✓ Časové omezení relace
  - ✓ Časové omezení spojení
- 11.6 Řízení přístupu k aplikacím a informacím
  - ✓ Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.
  - ✓ Omezení přístupu k informacím
  - ✓ Oddělení citlivých systémů

Skladba opatření ostatních kategorií řízení přístupu

- 11.7 Mobilní výpočetní zařízení a práce na dálku
  - ✓ Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a zařízení pro práci na dálku.
  - ✓ Mobilní výpočetní zařízení a sdělovací technika
  - ✓ Práce na dálku

Ilustrativní rozpis kategorie 11.4, Řízení přístupu k síti

- Cíl: Předcházet neautorizovanému přístupu k síťovým službám.
- Relevantní oblasti opatření
  - ✓ Politika používání síťových služeb
  - ✓ Autentizace uživatelů pro externí připojení
  - ✓ Identifikace zařízení v síti
  - ✓ Ochrana portů pro vzdálenou diagnostiku a konfiguraci
  - ✓ Princip oddělení v sítích
  - ✓ Řízení síťových spojení
  - ✓ Řízení směrování v síti
- Typová zabezpečovaná prostředí
  - ✓ privátní sítě na bázi pevných privátních spojů – WAN, LAN
  - ✓ VPN – alternativa WAN, na bázi protokolu IPSec ve veřejné síti (VPN pro vzdálený přístup, site-to-site VPN)
  - ✓ extranety – podpora B2B činností, VPN technologie
  - ✓ bezdrátové sítě – IEEE 802.11, Bluetooth, mobilní sítě, . . .

Politika používání síťových služeb

- Cíl – *Users shall only be provided with access to the services that they have been specifically authorized to use.*
- Politika určuje
  - ✓ které sítě a které síťové služby lze zpřístupňovat
  - ✓ adekvátní auutorizační procedury pro získání práva přístupu
  - ✓ která opatření musí chránit síťová připojení
- Politika musí vyhovovat politice řízení přístupu
- Bezpečnostní perimetr sítě vymezují směrovače a firewally
  - ✓ k aplikacím, údajům a službám běžícím v síti mohou přistupovat pouze autentizovaní uživatelé

Autentizace uživatelů pro externí připojení

- Cíl – *Appropriate authentication methods shall be used to control access by remote users.*
- Zranitelnost vzdáleného přístupu
  - ✓ vytáčená (komutovaná) spojení
  - ✓ bezdrátová spojení
- Bezpečný vzdálený přístup z internetu zajistí např. protokol Kerberos
- Na vytáčených spojeních lze použít zpětná volání

Identifikace zařízení v síti

- Cíl – *Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.*
  - ✓ nutné implementovat, pokud ohodnocení rizik indikuje, že je důležité zajistit, aby se relace otevírala pouze z konkrétního místa či počítače
  - ✓ např. bankovní přesuny peněz lze provádět pouze z . . .
- Nestačí znát adresu portu kabelu vedoucího k terminálu

Ochrana portů pro vzdálenou diagnostiku a konfiguraci

- Cíl – *Physical and logical access to diagnostic and configuration ports shall be controlled.*
  - ✓ vzdálený přístup si vynucuje požadavek možnosti konfiguračního nebo opravného zásahu
  - ✓ porty lze chránit fyzicky, zámkem, zpřístupnění podle ISMS procedury řeší obsluha počítače – po náležité autentizaci port na určenou dobu odemkne a učiní o tom auditní záznam

Princip oddělení v sítích

- Cíl – *Groups of information services, users, and information systems shall be segregated on networks.*
- Oddělení
  - ✓ Oddělení působností jisté služby může redukovat dopad narušení služby
  - ✓ Bezdrátové sítě mají být odděleny a s jinak bezpečnou zbývající sítí propojeny jediným bezpečným spojem (např. firewallem)
- Nutnost důkladné dokumentace
  - ✓ domén, rozmístění aktiv do domén, . . .

Řízení síťových spojení

- Cíl – *For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.*
  - ✓ spojení musí vyhovovat politice řízení přístupu
  - ✓ některá spojení mohou podléhat časovému plánu

Řízení směrování v síti

- Cíl – *Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.*
  - ✓ směrování musí vyhovovat politice řízení přístupu