Bezpečnostní dokumentace

1. Úvod – stručný popis účelu aplikace a jejích funkcí, komponent (HW, SW)

1.1 Popis dokumentu

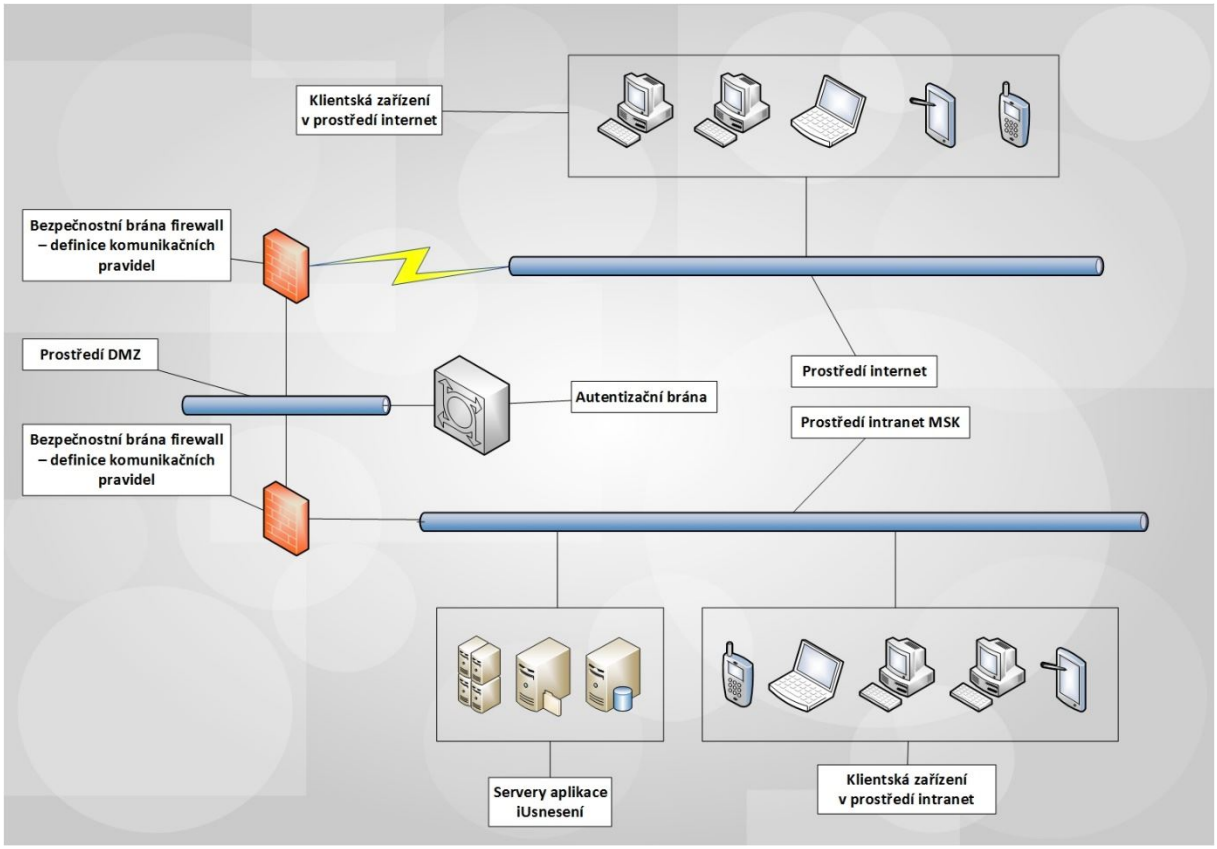
Dokument obecně popisuje bezpečnostní aspekty aplikace iUsnesení společnosti PilsCom, s.r.o.

1.2 Základy aplikace

Aplikace iUsnesení je aplikace pro zpracování materiálů samosprávy. Jedná se o webovou aplikaci. Jedinou výjimkou je klientská aplikace - doplněk aplikace Microsoft Word, který zpřístupňuje funkcionalitu editace materiálů v rámci prostředí Microsoft Word a umožňuje tak samotné editace materiálů. Jeho součástí je i ActiveX prvek, který umožňuje práci se soubory jednotlivých materiálů na klientských stanicích umístěných mimo interní síť MSK.

Uživatelsky je účelem aplikace zajištění práce a funkcí pro tvorbu a schvalování materiálů samosprávy, příprava programů jednání rady a zastupitelstva, hlasování o jednotlivých návrzích, zaznamenání výsledných schválených usnesení orgánů a jejich publikace. Podrobnější informace lze nalézt v uživatelské dokumentaci.

Z bezpečnostního hlediska je důležitá architektura na obr. 1



- Technicky je architektura samotné aplikace iUsnesení realizována pomocí tří serverů (či rolí), jejichž tabulka je uvedena níže:

Server	SW	Další údaje	Poznámka
Aplikační	MS Windows Server	IIS	
Databázový	MS Windows Server	MS SQL	
Dokumentový	MS Windows Server	Charon, FileNet P8, MS Sharepoint, MSSQL	

- Tyto servery mohou sdílet jeden až tři servery fyzické nebo virtuální. Verze produktů Microsoft (servery) se může odvíjet podle toho, jak bude probíhat certifikace nasazení jednotlivých verzí produktů v rámci ICT prostředí MSK.

- Složení aplikace z technického hlediska. Technicky se aplikace skládá z:

  - Obsahu aplikačního serveru, ASP.NET stránek. Tyto stránky jsou kompilované, jejich kód není obecně dostupný a neobsahuje aplikační logiku.

  - Databáze:

    - **iUsneseni**: obsahuje veškerá strukturovaná data o objektech aplikace

2. Bezpečnostní zásady

2.1.Důvěrnost, integrita a dostupnost objektů aplikace iUsnesení,

2.1.1 Odpovědnosti uživatelů za akce provedené v aplikaci

Platí zásada, že zodpovědnost je a vždy musí být dovozena ke konkrétnímu člověku.

Pod tímto přihlášení pracuje každý uživatel v aplikačním serveru IIS. Ten pracuje s databází pomocí nepřihlásitelného DB uživatele (je možné využití SQL login či NT Autentizace systémového účtu). Jméno přihlášení je všude, kde je to třeba uchováno v databázi.

- S aplikací iUsnesení nelze uživatelsky provést žádnou operaci včetně přihlášení do aplikace, není-li uživatel (fyz. osoba) platným způsobem přihlášen přes autentizační bránu. Poté jsou autentizační údaje uživatele předány v rámci web requestu do prostředí samotné aplikace.

- Aplikační server pracuje se stránkami vytvořenými v technologii Microsoft .NET. V takto napsaných stránkách je kód, jenž pracuje s databází iUsnesení v MS SQL.

- S touto databází pracuje aplikační server pod uživatelem DBO, pod nímž není možno se přihlásit. Tento uživatel se SQL autentizací či NT autentizací je vlastníkem právě databáze iUsnesení bez dalších oprávnění v rámci SQL Serveru. Musí mít default schéma **dbo** pro databázi iUsnesení.

- Dále aplikační server pracuje s úložištěm dokumentů. I s ním pracuje s uživatelem, pod nímž se nelze přihlásit a který je pro tuto roli vyhrazen. Úložiště dokumentů, resp.

nestrukturovaných dat je v případě využití integrovaného úložiště Charon (nativní součást iUsnesení) speciálním způsobem adresářově členěná oblast disku se souborovým systémem NTFS. To umožňuje důsledně granulovat systémová práva a auditovat přístup a manipulaci se soubory. Ukládají se sem jen soubory, které patří do aplikace iUsnesení. Přesně řečeno nejen soubory, ale i jejich verze. Jako úložiště pro nestrukturovaná data pak může být využito i úložiště databázové (content database) či DMS výrobců třetích stran – FileNet P8, Documentum, MS Sharepoint – aplikace splňuje standard CMIS pro případnou realizaci napojení DMS.

2.1.2 Nepopiratelnost, integrita a dostupnost služeb aplikace v bezpečnostním provozním módu s nejvyšší úrovní (do stupně utajení Důvěrné)

Zde bude uvedeno několik zásad, jimiž se realizují pravidla a zabezpečení přístupu.

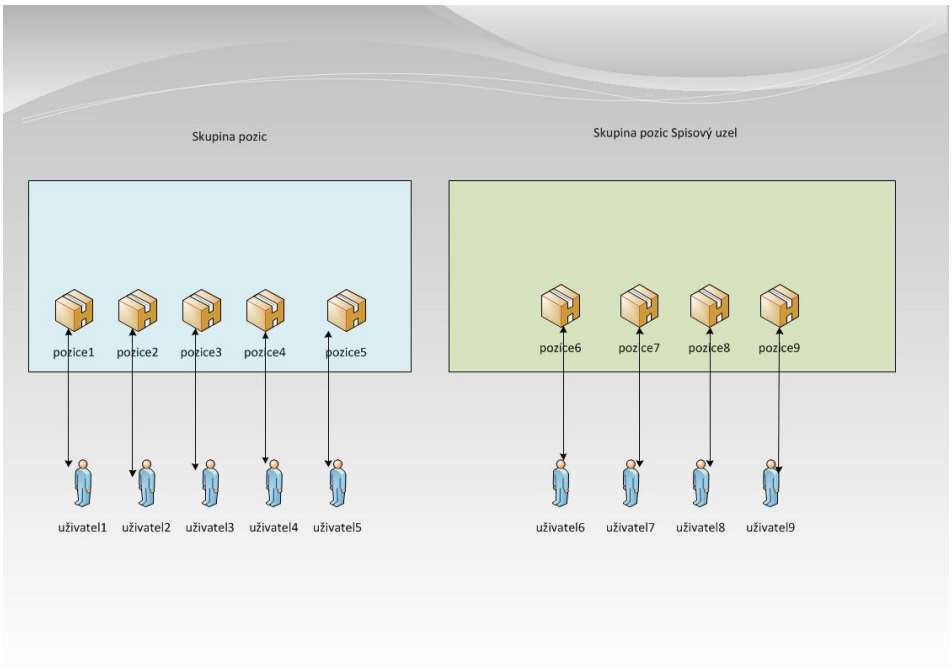
Odpovědnost je vždy na konkrétní osobě, která ale může vystupovat ve více rolích, které jsou představovány pozicemi.

🛠 Osoba je vždy a pouze objektově představována objektem uživatel v rámci aplikace a jeho uživatelským účtem.

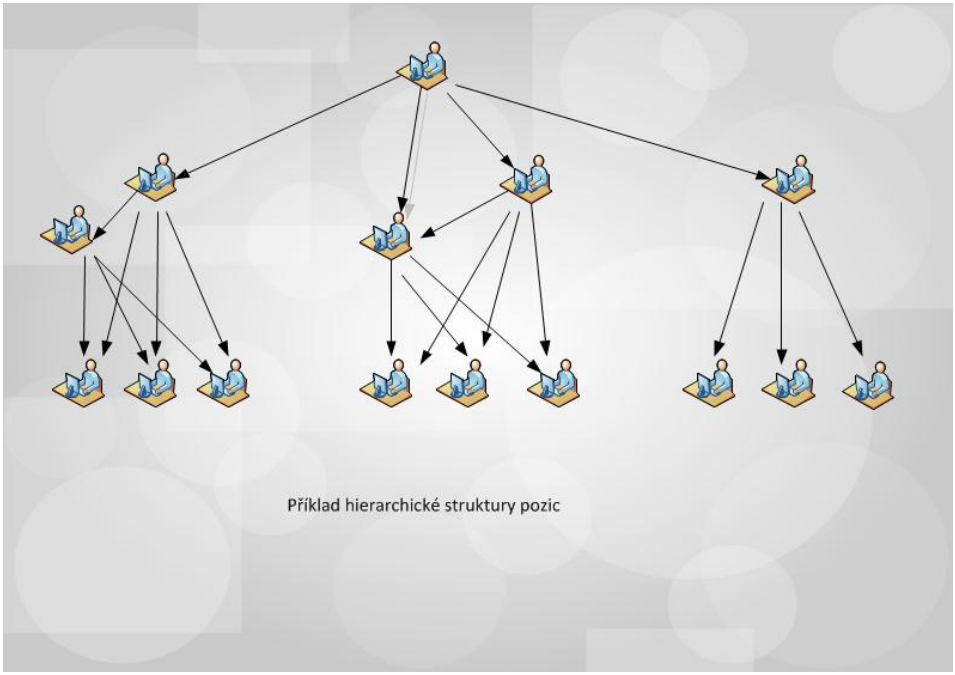
Pozice je de facto něco jako role, respektive pracovní místo. Aby mohl uživatel (tedy fyzická osoba) cokoliv vykonat v aplikaci iUsnesení, musí být jako uživatel přiřazen k určité pozici. Daný uživatel může být v určitém okamžiku přiřazen nanejvýš k jedné pozici.

🛠 Základní přiřazení uživatelů k pozicím provádí administrátor aplikace nebo plánovaná úloha napojení aplikace iUsnesení a IDM MSK. Případné zpřístupnění vlastní pozice nelze provést jinak, než jen zásahem administrátora (auditovaným) nebo spuštěním (auditovaným) plánované úlohy napojení aplikace iUsnesení a IDM MSK nebo proaktivně auditovanou akcí samotného vlastníka pozice.

Schématicky je to znázorněno na obrázku níže:



Pozice jsou při implementaci seřazeny do hierarchické struktury, jejíž příklad je na obrázku níže:



- V praxi lze ukázat příklad nepopiratelnosti odpovědnosti uživatele. Každý uživatel jakožto fyzická osoba autentizovaný přes autentizační bránu a s přístupem do aplikace má své vlastní přihlašovací jméno a heslo. Přidělení a odebrání tohoto účtu je věcí organizace a vnitřních předpisů organizace. Po aplikaci jména a hesla lze mít prokazatelně za to, že akci provedl např. Václav Novák.

- Dále provede některou akci, kterou mu jeho role umožňuje. Tato akce obnáší jednak operace v rámci webových stránek iUsnesení. Ty jsou zaznamenány pod jeho přihlašovacím jménem. V určitém okamžiku je ze stránky vyvolána databázová operace. Ta je v databázi provedena pod jménem vyhrazeného uživatele. Zároveň je zaznamenána do historie spolu s přihlašovacím jménem, názvem pozice a přesným časem. Tím je zajištěno spojení mezi uživatelem a operací, kterou provádí.

2.2.Minimální bezpečnostní požadavky

2.2.1. Zajištění jednoznačné identifikace a autentizace uživatele i pracovníků správy aplikace,

Uživatel je identifikován a autentizován prostředky autentizační brány. Tato určuje pouze fyzickou totožnost osoby. Strukturování práv k objektům aplikace je dáno její vnitřní logikou a je popsáno dále.

Aplikace může seskupovat pozice do skupin. Další způsob seskupení pozic je do spisových uzlů, které se shodují zpravidla s organizačním členěním.

- Skupiny pozic a spisové uzly jsou realizovány prakticky totožně, názvová diference má pouze metodický charakter.

V aplikaci iUsnesení je právo přístupu přiděleno už od vstupu materiálu (jeho první verze) do systému.

Následně jsou práva definována v rámci přiřazeného workflow a to vždy tak, že právo autora má pozice, kde se materiál v rámci běhu workflow právě nachází. Každé workflow má vždy spojitost s konkrétním spisovým uzlem a odpovídající hierarchií pozic v rámci spisového uzlu.

Vedoucí oddělení a vedoucí odboru má právo čtenáře na všechny materiály podřízených pozic.

Pro každé jednotlivé workflow je taktéž definována skupina pozic, která zajišťuje právo na materiály konkrétního spisového uzlu a to s oprávněním čtenáře. Členství pozic v této skupině určuje administrátor aplikace.

Platí taktéž, že právo čtenáře má vždy každá pozice, přes kterou materiál, při průchodu grafem workflow, prošel – jedná se o takzvané dotčené materiály.

Správce sekce má oprávnění čtenáře na všechny materiály, které spadají pod jím spravovanou sekci, přičemž sekcí se rozumí orgán organizace (rada, zastupitelstvo, komise, výbor).

Supervizor aplikace má oprávnění čtenář na všechny materiály ve všech sekcí v rámci aplikace.

Administrátor aplikace má oprávnění provádět administrativní kroky v rámci aplikace – tímto se rozumí například vytváření zástupů, přiřazení oprávnění jednotlivých pozic či skupin pozic, definice některých systémových proměnných, správa plánovaných úloh aplikace, kontrola odesílaných emailů,…

Vyhodnocení způsobilosti

Vyhodnocení způsobilosti je součástí každého přístupu. Míra a čas způsobilosti je u pozice i u uživatele. Obecně se nemusí shodovat. Dále je zaveden pojem: **Způsobilost logonu**.

Typy přístupů k objektům jsou žádný, čtenář, autor, vlastník.

2.2.2. Nepřetržité zaznamenávání bezpečnostně relevantních událostí do auditních záznamů a zajištění jejich ochrany

Bezpečnostně relevantní události vznikají na těchto úrovních:

- Aplikační logikou, tedy velkou řadou událostí, které vznikají činností uživatelů, administrací i provozem. Tyto události jsou zaznamenávány v reálném čase do databáze ve strukturovaném formátu jako záznamy v tabulce databáze.
- Událostmi databáze, zejména vznik, modifikace, mazání objektů databáze. Tyto události lze nasměrovat jak do databáze samotné, tak do systémového EventLogu do Security části.
- Událostmi Windows. Ty se zaznamenávají do systémového Eventlogu.

🛠 Výše uvedené zásady jsou zajištěny následovně:

- 🛠 Aplikační log se v terminologii aplikace iUsnesení nazývá záznam historie. Tyto události jsou uvedeny v tabulce: AA_Slozkahistorie.
- 🛠 Změny v databázi jsou monitorovány a zaznamenávány pomocí Auditlog:
- 🛠 Tímto způsobem jsou logovány následující tabulky:
    - AA_dokument (záznamy o souborech u materiálů, návrhů, usnesení),
    - AA_dokumentverze (záznamy o verzích souborů),
    - US_UseseniNavrh (záznamy o materiálech),
    - US_UsneseniJednani (záznamy o jednotlivých jednáních orgánů),
    - WF_Workobject, WF_WorkobjectStep, WF_WorkObjectStepMove (záznamy o běhu jednotlivých workflow),
    - AA_slozkahistorie (aplikační auditní záznamy)
- 🛠 Výstupy AuditlLog jsou směrovány do EventLog MS Windows Server. Správce databáze je nemůže modifikovat.

2.2.3. Možnost zkoumání auditních záznamů a stanovení odpovědnosti konkrétního uživatele

Auditní záznamy aplikace iUsnesení může zkoumat administrátor aplikace. Veškeré události se vždy zaznamenají s jednoznačnou identifikací, který uživatel je za ně zodpovědný.

- 🛠 Pokud by se je pokusil modifikovat, pak se o tom objeví záznam v AuditLog databáze. Ten je přístupný jen bezpečnostnímu manažeru.

Pokus o případnou modifikaci auditních záznamů aplikace je zaznamenán v auditním logu databáze. Tento log je nasměrován do eventlogu Windows.

Auditování MSSQL:

Nejprve je potřeba pomocí sql server management studia vytvořit objekt samotného auditu – toto je možné provést pomocí sql skriptu - v tomto případě jsou audit events směrovány do security systémového logu – další možnosti jsou eventy směrovat do aplikačního systémového logu nebo do souborového logu filesystémové úložiště. V příkladovém skriptu je taktéž nastaveno, aby v případě selhání auditování (místo na disku, zaplněný soubor event logu) server zůstal v běhu – je možné nastavit tak, aby došlo k shutdown serveru:

```
USE [master]
GO

CREATE SERVER AUDIT [AuditiUsneseni]
TO SECURITY_LOG
WITH
(     QUEUE_DELAY = 10000
      ,ON_FAILURE = CONTINUE)
GO
```

Následně je potřeba vytvořit objekt audit specification nad konkrétní databází aplikace iUsnesení:

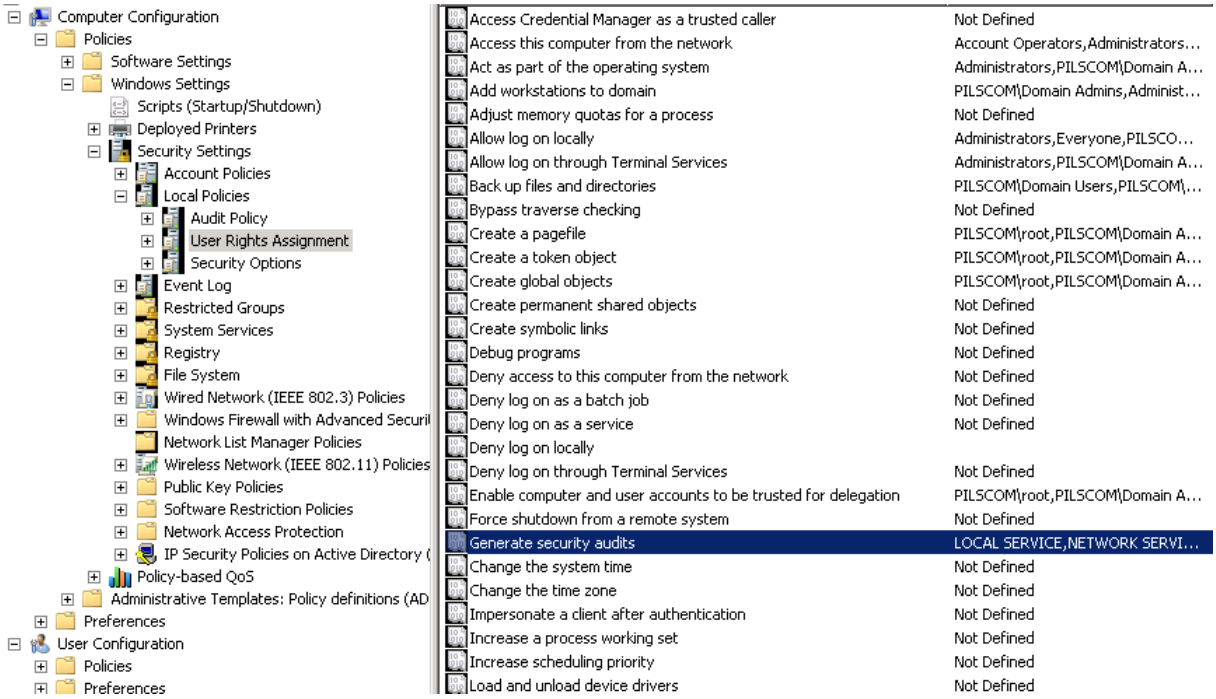
```
USE [iUsneseni]
GO

CREATE DATABASE AUDIT SPECIFICATION [iUsneseni_PI_Dok_DokVer]
FOR SERVER AUDIT [AuditiUsneseni]
ADD (DELETE ON OBJECT::[dbo].[AA_Dokument] BY [dbo]),
ADD (INSERT ON OBJECT::[dbo].[AA_Dokument] BY [dbo]),
ADD (UPDATE ON OBJECT::[dbo].[AA_Dokument] BY [dbo]),
ADD (DELETE ON OBJECT::[dbo].[AA_DokumentVerze] BY [dbo]),
ADD (INSERT ON OBJECT::[dbo].[AA_DokumentVerze] BY [dbo]),
ADD (UPDATE ON OBJECT::[dbo].[AA_DokumentVerze] BY [dbo]),
ADD (DELETE ON OBJECT::[dbo].[US_UsneseniNavrh] BY [dbo]),
ADD (INSERT ON OBJECT::[dbo].[US_UsneseniNavrh] BY [dbo]),
ADD (UPDATE ON OBJECT::[dbo].[US_UsneseniNavrh] BY [dbo]),
ADD (DELETE ON OBJECT::[dbo].[US_UsneseniJednani] BY [dbo]),
ADD (INSERT ON OBJECT::[dbo].[US_UsneseniJednani] BY [dbo]),
ADD (UPDATE ON OBJECT::[dbo].[US_UsneseniJednani] BY [dbo]),
ADD (DELETE ON OBJECT::[dbo].[WF_Workobject] BY [dbo]),
ADD (INSERT ON OBJECT::[dbo].[WF_Workobject] BY [dbo]),
ADD (UPDATE ON OBJECT::[dbo].[WF_Workobject] BY [dbo]),
ADD (DELETE ON OBJECT::[dbo].[WF_WorkobjectStep] BY [dbo]),
ADD (INSERT ON OBJECT::[dbo].[WF_WorkobjectStep] BY [dbo]),
ADD (UPDATE ON OBJECT::[dbo].[WF_WorkobjectStep] BY [dbo]),
ADD (DELETE ON OBJECT::[dbo].[WF_WorkobjectStepMove] BY [dbo]),
ADD (INSERT ON OBJECT::[dbo].[WF_WorkobjectStepMove] BY [dbo]),
ADD (UPDATE ON OBJECT::[dbo].[WF_WorkobjectStepMove] BY [dbo])
WITH (STATE = ON)
GO
```

Poté již stačí v prostředí MSSQL Serveru audit povolit:

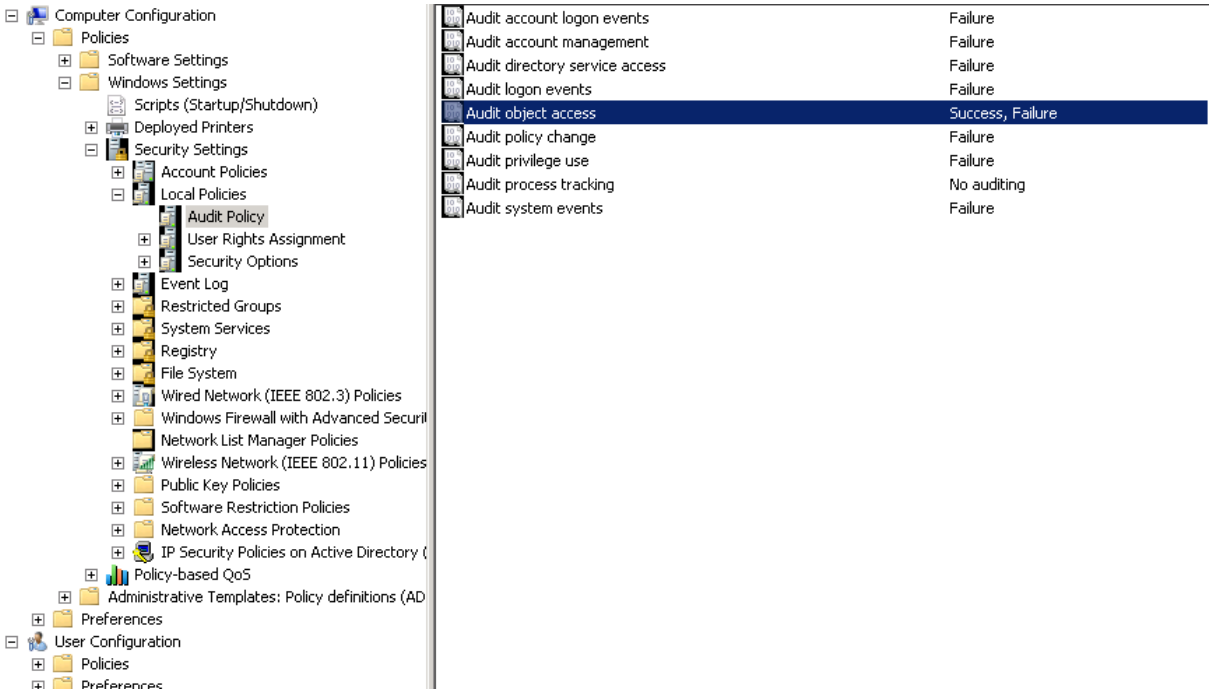
```
use master
go
alter server audit AuditiUsneseni
with (state=on)
go
```

Poté je třeba zajistit, aby uživatel služby MSSQL serveru měl dostatečná práva v rámci systému – je požadováno oprávnění Generate security audits – lze definovat v rámci group policy:



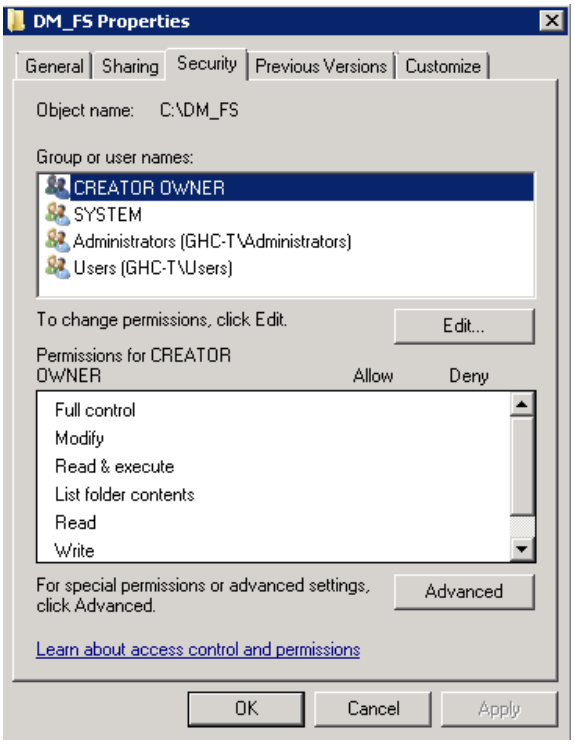
Defaultně je toto oprávnění povoleno pro systémové účty Network Service a Local Service.

Je taktéž potřeba zajisti logování Succes i Failur audits events – toto zajistíme taktéž pomocí group policy objektu, kde je třeba pro daný server nastavení propagovat:

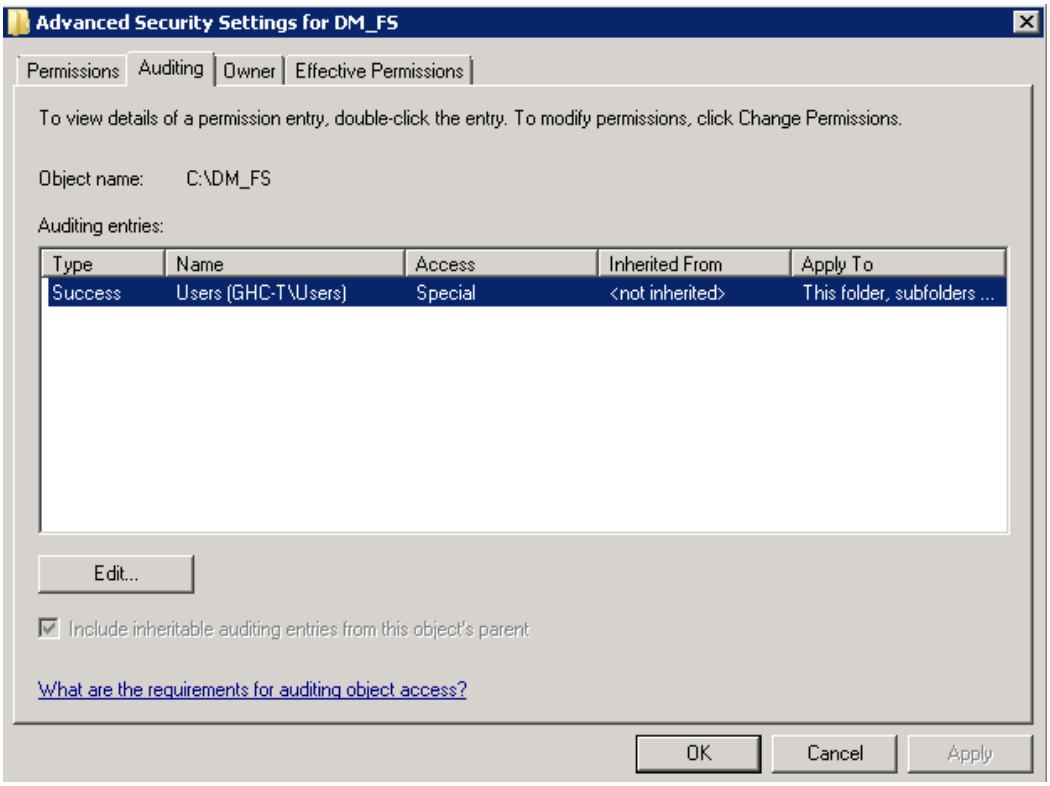


Auditování NTFS (vhodné pro úložiště nestrukturovaných dat Charon):

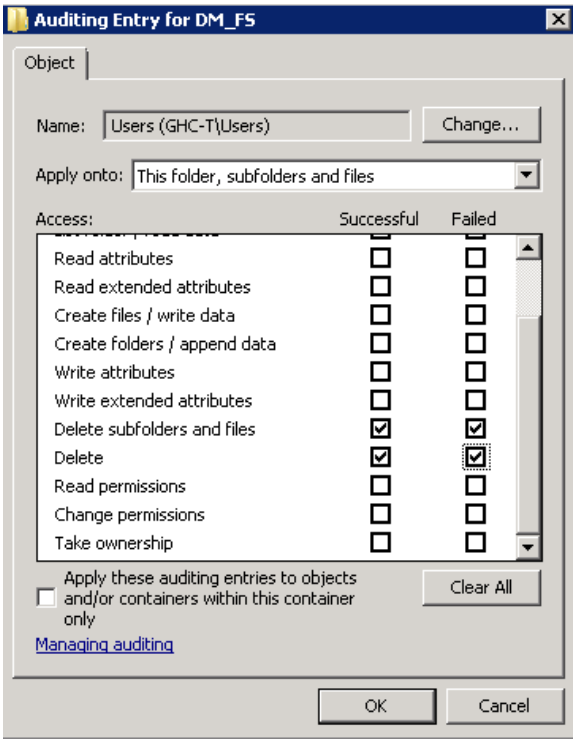
Auditování nastavíme nad konkrétním adresářem - v rámci Security vybereme možnost Advanced.



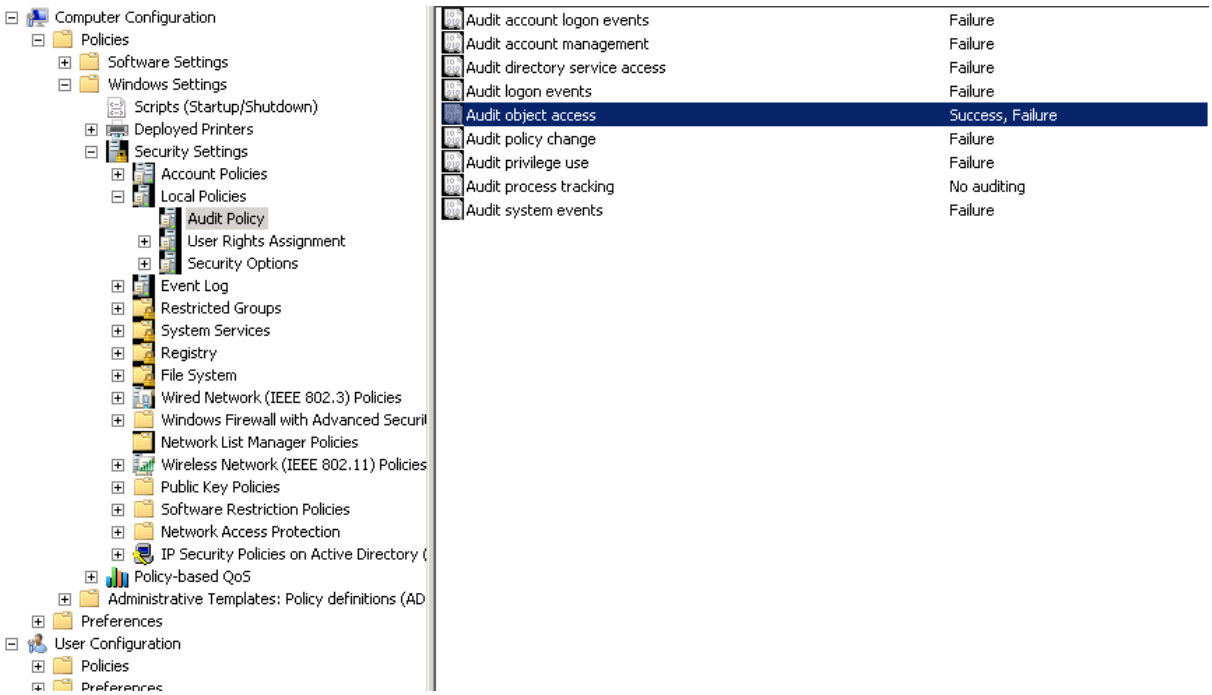
Vybereme Auditing a Edit…



Nadefinujeme skupinu uživatelů, jejichž činnost nad adresářem se má sledovat a vybereme auditované události.



Je taktéž potřeba zajisti logování Success i Failure audits events – toto zajistíme taktéž pomocí group policy objektu, kde je třeba pro daný server nastavení propagovat:



Je potřeba počítat s tím, že součástí běžných operací nad úložištěm je i strojové odmazávání adresářů – toto se děje vždy v rámci nadřazeného adresáře _LastFolder. V ostatních částech adresářové struktury za běžných okolností ke smazání objektů nedochází.

2.2.4. zajištění nepopiratelnosti – jakými funkcemi

Nepopiratelnost odpovědnosti je soubor principů, kdy lze jednoznačně dovodit odpovědnost konkrétního uživatele. Základním parametrem je uživatelské jméno, které uživatel použije pro přihlášení do sítě (autentizační brána) a následně do aplikace. Toto jméno je jak v auditních záznamech, tak v aplikačním logu v databázi.

2.3.Požadavky fyzické bezpečnosti pro HW komponenty

Systém aplikace iUsnesení se skládá z následujících HW komponent:

- Serverové
  - Aplikační server
  - Databázový server
  - Datový server
- Klientské
  - Klientská zařízení (počítače, tablety,…)

Serverové komponenty jsou používány plně v režimu sítě organizace a aplikace iUsnesení nevyžaduje žádnou její změnu.

Komunikace mezi klientským zařízením a serverovou částí aplikace se provádí vždy přes autentizační bránu a v rámci zabezpečeného připojení (protokol https). Toto se týká jak práce se samotnou webovou částí aplikace, tak i při navazování spojení z aplikace Microsoft Word (doplněk aplikace iUsnesení).

Samotná editační práce se soubory jednotlivých návrhů se pak liší podle umístění klientských zařízení a dá se rozdělit na dvě prostředí:

- Prostředí intranet
- Prostředí internet

Prostředí intranet

V prostředí intranetu probíhá editační práce se soubory jednotlivých návrhů tak, že komunikace a autentizace uživatele je řízena přes autentizační bránu a přes zabezpečený protokol https. Samotná práce se souborem pak probíhá přes Windows Share, kdy tento je zpřístupněn uživateli v samostatném podadresáři adresáře sdíleného. Na tento podadresář je pak aplikací iUsnesení aplikován, přímo na souborový systém serveru NTFS, ACL (přístupový list), který zajišťuje přístup do tohoto podadresáře pouze uživateli, který se souborem pracuje. Ostatním uživatelům (s výjimkou lokálních administrátorů Windows Serveru) je přístup do tohoto podadresáře zakázán. Samotná editace se pak provádí v prostředí aplikace Microsoft Word.

Prostředí internet (extranet)

V prostředí internetu probíhá editační práce se soubory jednotlivých návrhů tak, že komunikace a autentizace uživatele je řízena přes autentizační bránu a přes zabezpečený protokol https. Práce se souborem pak probíhá tím způsobem, že tento je stažen do temp adresáře uživatele respektive do adresářové struktury, která je v tomto adresáři vytvořena. Stažení probíhá přes webovou cestu respektive přes HTTPS protokol a tento požadavek je prováděn vždy s odpovídající autentizací uživatele. Po provedení potřebných úprav v prostředí aplikace Microsoft Word je soubor přes webovou cestu odeslán do aplikace, kde dojde k vytvoření nové verze. Následně, při uzavření prostředí aplikace Microsoft Word, je soubor odstraněn z temp adresáře uživatele.

2.4.Role ve správě vyžadované pro aplikaci, školení uživatelů

Role se skládá z práv, které jsou dělitelné do základních skupin – základní, rozšířené, administrátoři.

Tabulka níže definuje základní sadu školení, která bývá implementována při náběhu systému:

Název	délka	Cílová skupina	Poznámka
základní	Půl dne	Většina uživatelů	
rozšířené	1 den	Správci jednání	
Administrátorské	1 den	Administrátoři aplikace	