Smlouva o dílo

uzavřená podle § 2586 násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Číslo smlouvy SD2400251

Objednatel:

Název společnosti:	**ZDRAVOTNÍ ústav se sídlem v Ústí nad Labem**
Sídlo:	Moskevská 1531/15, 400 01 Ústí nad Labem
zastoupená:	Ing. Eduardem Ježem, ředitelem, na základě jmenování čj. MZDR 18286/2021-4/PER ze dne 14. 5. 2021
IČ: 71009361	
Bankovní spojení:	Číslo účtu

Jako objednatel na straně jedné (dále také jako „objednatel“)

a

Zhotovitel:

Název společnosti:	**Mepatek s.r.o.**
Sídlo:	U divadla 25, 415 01 Teplice
zastoupená:	Danielou Dohnalovou, jednatelem společnosti
IČ: **27268080**	DIČ: CZ27268080
Bankovní spojení:	číslo účtu

Společnost vedená u Krajského soudu v Ústí nad Labem spis. značka C 21540.

Jako zhotovitel na straně druhé (dále také jako „zhotovitel“)

prohlašují, že jsou zcela způsobilí k právním úkonům a po vzájemné domluvě uzavírají tuto smlouvu:

I. Předmět smlouvy

1. Předmětem smlouvy je dodávka a implementace technologií pro zvýšení kybernetické bezpečnosti informačních systémů a komunikačních systémů objednatele pro zakázku VZ0182279: ZUUL – Zvýšení kybernetické bezpečnosti.

II. Specifikace dodávky

1. Zhotovitel se zavazuje k dodávce komodit K1 a K2, zvýšení zabezpečení komunikační sítě, nástroje pro zajišťování úrovně dostupnosti informací.

2. Obsah dodávky je uveden v příloze 4268543-Příloha 5 ZD - Podrobná specifikace předmětu plnění a požadavky na realizaci zakázky, část tech. kvalifikace_3v0.

Dále jen „Dodávka“.

III. **Termín plnění**

1. Plnění bude zahájeno po podpisu této smlouvy.

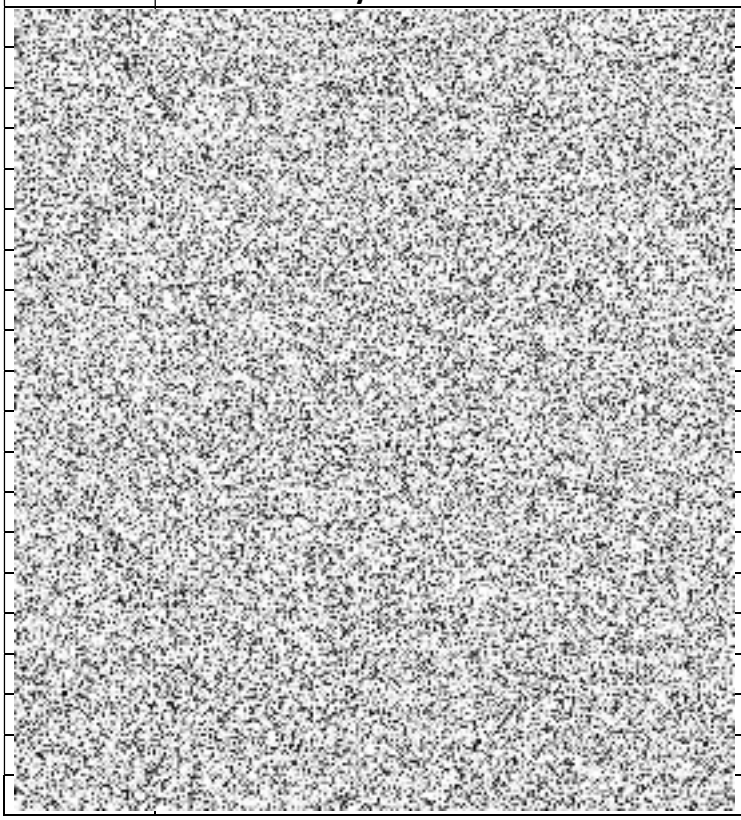
2. Termín ukončení předmětu veřejné zakázky je 200 dní od podpisu této smlouvy.

3. Harmonogram

Etapa 1 - dodávky a implementace K.1-K.3		
E1.1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D+60
E1.2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+60
E1.3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+65
E1.4	Dodávka HW a licencí	D+80
E1.5	Implementace řešení	D+160
E1.6	Školení uživatelů a administrátorů	D+180
E1.7	Zkušební provoz	D+190
E1.8	Akceptační testy a předání	D+200

IV. **Místo plnění**

1. Místem plnění jsou pracoviště Zdravotního ústavu se sídlem v Ústí nad Labem:

Lokalita	**Adresa lokality**
	

V. **Cena za dílo**

1. Cena je stanovena za kompletní provedení předmětu veřejné zakázky a je stanovena jako nejvýše přípustná za splnění celého předmětu veřejné zakázky v příloze 4188656-Příloha 1 ZD - Krycí list nabídky.

2. Cena za dodávku specifikovanou v bodě 3 této smlouvy je **8 170 004 Kč** bez DPH,

3. Výše DPH **1 715 700,84Kč**. Dodávka je v základní sazbě 21 %.

4. Celková cena za celý předmět veřejné zakázky **9 885 704,84 Kč** včetně DPH.

VI. Komunikace, pravomoci a odpovědnosti zástupců smluvních stran

1. Kontaktní osoby

   a. Kontaktní osoba Zhotovitele:

   Účel – provozní záležitosti
   Jméno, Příjmení:
   e-mail:

   b. Kontaktní osoba Zhotovitele:

   Účel - finanční záležitosti
   Jméno, Příjmení:
   e-mail:

   c. Kontaktní osoba Objednatele:

   Účel - provozní, finanční záležitosti
   Jméno, Příjmení:
   e-mail:
   a
   k

2. Oprávněné osoby, jsou zplnomocněné osoby smluvních stran, které jsou oprávněny jednat jménem smluvních stran o všech smluvních a obchodních záležitostech týkajících se Smlouvy a souvisejících s jejím plněním.

   a. Oprávněné osoby Zhotovitele:

   Jméno, Příjmení:
   e-mail:

   b. Oprávněné osoby Objednatele:

   Jméno, Příjmení:
   e-mail:

3. Odpovědné osoby, jsou pracovníci smluvních stran pověření jednáním jménem smluvních stran v otázkách plnění Smlouvy.

    a. Oprávněné osoby Zhotovitele:

    Jméno, Příjmení:
    e-mail:
    

    b. Oprávněné osoby Objednatele:

    Jméno, Příjmení:
    e-mail:
    

VII. **Platební podmínky**

1. Cena bude Objednatelem Zhotoviteli zaplacena na základě vystavení faktury Zhotovitelem a jejím doručení Objednateli. Zhotovitel je oprávněn vystavit fakturu vždy po úspěšném předání a převzetí předmětu plnění prostého vad a nedodělků. Cena bude Objednatelem zaplacena bankovním převodem na účet Zhotovitele uvedený na faktuře.

2. Vystavenou fakturu doručí Zhotovitel do 3 (*slovy: tří*) dnů ode dne jejího vystavení Objednateli, a to v elektronické podobě na adresu . Zhotovitel souhlasí s použitím faktur v elektronické podobě dle § 26 odst. 3 zák. č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

3. Faktura je splatná do 60 (*slovy: šedesát*) dnů od jejího prokazatelného doručení Objednateli.

4. Objednatel se zavazuje potvrdit přijetí faktury elektronicky na email .

5. Faktura musí obsahovat náležitosti daňových dokladů v souladu s příslušnými obecně závaznými právními předpisy.

6. Faktura musí obsahovat text „plnění k projektu Zvýšení kybernetické bezpečnosti Zdravotního ústavu se sídlem v Ústí nad Labem, registrační číslo CZ.06.01.01/00/22_003/Q000035, realizovaného v rámci Integrovaného regionálního operačního programu 2021–2027 spolufinancovaného Evropskou Unií a ke smlouvě SD2400251“.

7. Nebude-li faktura Zhotovitele obsahovat všechny zákonem stanovené náležitosti nebo bude-li obsahovat nesprávné údaje nebo bude-li vystavena neoprávněně, je Objednatel povinen ji bezodkladně, nejpozději však do 7 (*slovy: sedmi*) pracovních dnů vrátit Zhotoviteli spolu s odůvodněním, proč je faktura nesprávně či neoprávněně vystavena.

Zhotovitel může po odstranění vad, či po vzniku svého oprávnění zaslat Objednateli fakturu novou či opravenou; vždy však s novou lhůtou splatnosti fakturované částky v souladu s čl. 7.3 této Smlouvy.

VIII. **Prohlášení Zhotovitele**

1. Zhotovitel tímto prohlašuje a ujišťuje objednatele že:

   - je plně odborně způsobilý k poskytování Služeb dle této Smlouvy a je schopen jednat se znalostí a pečlivostí, která je s touto odborností spojena dle příslušných ustanovení Občanského zákoníku.
   - udržuje a po celou dobu trvání této Smlouvy bude udržovat v platnosti, jsou-li potřebné, technologické certifikace, licence, souhlasy, povolení a oprávnění potřebná k plnění svých povinností dle této Smlouvy a nehrozí, že by platnost takové licence, souhlasu, povolení a/nebo oprávnění bylo ukončeno.

IX. **Práva a povinnosti Zhotovitele**

1. Zhotovitel se zavazuje řídit se pokyny Objednatele a dodržovat lhůty pro poskytnutí Služeb stanovené v této Smlouvě a/nebo dohodnuté s Objednatelem. Zhotovitel je povinen upozornit na případnou zřejmou nevhodnost pokynů Objednatele, které by mohly mít za následek vznik újmy. V rámci Analýzy nasazení budou stanoveni garanti s oprávněním nahlašovat problémy

2. Zhotovitel je povinen při poskytování Dodávky postupovat s odbornou péčí a v nejlepším zájmu Objednatele. Zhotovitel je povinen při poskytování Služeb dodržovat zejména platné právní předpisy a technické normy.

3. Zhotovitel je oprávněn k plnění svých povinností použít třetí osobu, a to firmu Aricoma Systems a.s., IČ: 04308697. Zhotovitel za třetí osobu odpovídá jako by Dodávku poskytoval sám.

4. Zhotovitel je povinen uchovávat veškerou dokumentaci související s realizací Dodávky včetně účetních dokladů minimálně do 31. 12. 2035.

5. Zhotovitel je povinen minimálně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (Centra, MMR, MF, Evropské komise, Evropského účetního dvora (dále také „EÚD“), Nejvyššího kontrolního úřadu (dále také „NKÚ“), příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

6. Zhotovitel je povinen a zavazuje se při poskytování Dodávky vynaložit veškeré úsilí, aby nezpůsobil, případně odvrátil, hrozící újmu Objednateli, o které se při výkonu své činnosti ve vztahu k Objednateli dozví.

7. Zhotovitel je povinen poskytovat Dodávky Objednateli v dohodnutých lhůtách, v souladu s touto Smlouvou, příslušnými právními předpisy, technickými normami tak, aby byly způsobilé pro užití k obvyklému účelu, a průběžně informovat Objednatele o postupu v jejich řešení. Zhotovitel je povinen Objednatele bezodkladně písemně

upozornit na počínající prodlení s poskytováním Služeb, příp. požádat o možnost prodloužení Lhůty k poskytnutí služby.

8. V případě, že výstupy Dodávky vykazují vady, je Zhotovitel povinen je odstranit, a to bez zbytečného odkladu poté, co byl na jejich výskyt Objednatelem upozorněn. Objednatel musí vady Služeb vytknout Zhotoviteli nejpozději do 3 (slovy: tří) pracovních dnů ode dne, co se o nich dozvěděl, a to jakýmkoliv způsobem, např. telefonicky, e-mailem nebo ústně.

X. **Povinnosti Objednatele**

1. Objednatel se zavazuje poskytnout Zhotoviteli součinnost nezbytnou pro řádné plnění povinností Zhotovitele dle této Smlouvy a předat mu veškeré informace a podklady nezbytné pro poskytování Služeb dle této Smlouvy.

2. Zjistí-li Objednatel, že Zhotovitel poskytuje Služby v rozporu se svými povinnostmi a nedodržuje příslušná ustanovení Smlouvy, je Objednatel oprávněn vůči Zhotoviteli uplatnit práva z vadného plnění a požadovat, aby Zhotovitel poskytoval Služby řádným způsobem. Objednatel musí práva z vadného plnění uplatnit do 6 (slovy: šesti) měsíců od poskytnutí Služby, jinak právo zaniká.

3. Předmětem této smlouvy je dále i zajištění a sjednání podmínek vzdáleného přístupu zhotovitele bez aktivní účasti objednatele do prostředí objednatele za účelem plnění této smlouvy.

4. Objednatel se zavazuje, že umožní zhotoviteli vzdálený přístup k serverovému a síťovému prostředí za účelem plnění této smlouvy nejpozději do 10 pracovních dnů ode dne uzavření této smlouvy.

XI. **Mlčenlivost a ochrana osobních údajů**

1. Zhotovitel se zavazuje zachovávat mlčenlivost o veškerých informacích organizačního, technického, personálního, bezpečnostního, obchodního, nebo jiného interního charakteru, týkajících se Objednatele, zejména, nikoliv však výlučně, informací o jakýchkoli postupech (výrobních, zkušebních, prodejních apod.), o obchodních nebo marketingových plánech, koncepcích a strategií, záměrech a kalkulacích, obchodní strategii, o identitě klientů, spolupráci s klienty, o nakládání s financemi, o know-how, o provozních metodách, procedurách a pracovních postupech, o identitě třetích osob spolupracujících s Objednatelem, informacích o vztazích s obchodními partnery nebo o pracovněprávních otázkách, o cenách a podnikatelských příležitostech Objednatele, včetně dalších informací majících charakter obchodního tajemství (dále jen „Důvěrné informace“). Smluvní strany považují Důvěrné informace dle předchozí věty za obchodní tajemství a zavazují se s nimi nakládat jako s obchodním tajemstvím, přičemž se Zhotovitel zejména zavazuje je uchovávat v tajnosti, učinit veškerá opatření zabraňující jejich zneužití a/nebo prozrazení a/nebo neužít je v rozporu s účelem této Smlouvy a/nebo pro svůj vlastní prospěch a/nebo za účelem převádění klientů a zaměstnanců Objednatele. Objednatel je oprávněn Zhotoviteli výslovně určit, které informace považuje za Důvěrné informace ve smyslu této Smlouvy.

2. Zhotovitel se dále zavazuje zajistit zachovávání mlčenlivosti u veškerých svých zaměstnanců a třetích osob, kterých k plnění povinností dle této Smlouvy užije, a to minimálně ve stejném rozsahu.

3. Zhotovitel se zavazuje, že nebude Důvěrné informace užívat, kopírovat, shromažďovat nebo jinak dále reprodukovat nebo uchovávat ve vlastních či jiných databázích či jiných obdobných programech, ani je nebude šířit, zpřístupňovat ani předávat jakékoli třetí osobě. To neplatí v případě informací (i) k jejichž zpřístupnění dostane Zhotovitel písemný souhlas Objednatele, (ii) poskytnutých třetím osobám, které použije k plnění svých povinností podle této Smlouvy vázaných povinností mlčenlivosti minimálně ve stejném rozsahu, (iii) jejichž zpřístupnění je vyžadováno právním předpisem nebo závazným rozhodnutím orgánu veřejné moci nebo (iv) pokud Objednatel již danou informaci zveřejnil nebo pokud (v) tato informace byla již obecně známá bez ohledu na jednání Zhotovitele a jeho zavinění.

4. Smluvní strany se dále zavazují zachovávat mlčenlivost o obsahu této Smlouvy a nesdělit její obsah jakékoli třetí osobě.

5. Smluvní strany sjednávají, že povinnost mlčenlivosti uvedená v tomto článku Smlouvy není dotčena ukončením poskytování služeb dle této Smlouvy ani ukončením účinnosti této Smlouvy z jakéhokoliv důvodu, a tedy trvá v plném rozsahu i po ukončení účinnosti této Smlouvy, ledaže Objednatel Zhotovitele této povinnosti písemně zcela, nebo jen částečně, zprostí.

6. Smluvní strany se zavazují, že budou plnit všechny povinnosti vyplývající z právních předpisů na ochranu osobních údajů. Objednatel bere na vědomí, že Zhotovitel bude v souvislosti s poskytováním Služeb podle této Smlouvy za účelem splnění této Smlouvy provádět zpracování osobních údajů poskytnutých mu Objednatelem o Objednateli a jeho zaměstnancích. Objednatel se zavazuje informovat své zaměstnance a třetí osoby pro něj pracující o zpracovávání osobních údajů Zhotovitelem a věcech s tím souvisejících. Zhotovitel není oprávněn údaje poskytnout třetím osobám s výjimkou případu, kdy je taková povinnost stanovena zákonem, a dále v případech, kdy na základě smluvního ujednání třetí osoba údaje pro Zhotovitele zpracovává. O takových třetích osobách Zhotovitel informuje Objednatele. Zhotovitel se zavazuje zajistit ochranu těchto osobních údajů před zneužitím.

XII. **Záruka**

1. Záruka na části díla jako funkční celky.

- Zhotovitel poskytuje záruku na jednotlivé části díla jako na funkční celky, které mají plnit požadavky na zvýšení kybernetické bezpečnosti objednatele stanovené v této smlouvě a jejích přílohách.
- Zhotovitel poskytuje objednateli záruku v délce trvání 2 let. Jednotlivé části díla dle této smlouvy budou ke dni předání a převzetí objednatelem způsobilé k řádnému užití a budou mít vlastnosti stanovené touto smlouvou.
- Zhotovitelem poskytovaná záruka se vztahuje na kompletní funkčnost jednotlivých částí díla, jakož i na jejich vlastnosti požadované objednatelem.
- Záruční doba začíná běžet ode dne převzetí jednotlivé části nebo celého díla objednatelem.

- Veškeré zjištěné nedostatky, nedodělky a vady díla, které se vyskytnou v záruční době, je objednatel povinen bez zbytečného odkladu písemně oznámit zhotoviteli.
- Vadou díla se pro účely této smlouvy rozumí rozpor mezi sjednanými podmínkami provedení díla, jeho parametry a skutečným stavem díla.
- Objednatel má vůči zhotoviteli tato práva z odpovědnosti za vady:
    - právo na bezplatné odstranění reklamovaných vad, a to v nejkratším možném termínu po oznámení vady objednatelem
    - právo na odstoupení od smlouvy, kdy vady či nedodělky jsou takového charakteru, že ztěžují či dokonce brání v užívání díla, nebo
    - právo na zaplacení nákladů na odstranění vad v případě, kdy si objednatel vadu či nedodělek odstraní sám nebo použije třetí osoby k jejich odstranění, dohodli-li se tak se zhotovitelem.
- Uplatněním nároků z odpovědnosti za vady není dotčeno právo na náhradu škody. Zhotovitel odpovídá objednateli za případnou škodu, která mu vznikne z titulu neodstranění vady díla zhotovitelem ve stanoveném termínu.
- Záruka je poskytována v souladu s ustanovením § 2113 a násl. zákona č. 89/2012 Sb., občanského zákoníku, v platném znění.

2. Záruka na zařízení - na jednotlivá zařízení, která budou dodána jako součást částí díla, čí díla jako celku, je záruka definována v příloze Příloha 5 ZD - Podrobná specifikace předmětu plnění a požadavky na realizaci zakázky, část tech. kvalifikace_3v0 této smlouvy specificky. Jedná se typicky o záruku a záruční servis výrobce daného zařízení a technologie, kterou je možné odebrat a dodat jako příslušenství

XIII. **Závěrečná ustanovení**

1. Tato Smlouva nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti dnem jejího zveřejnění v informačním systému registru smluv zřízeném podle zákona číslo 340/2015 Sb. ve znění pozdějších předpisů.

2. Tato Smlouva je v souladu s obchodními a platebními podmínkami uvedenými v zadávací dokumentaci veřejné zakázky VZ0182279: ZUUL – Zvýšení kybernetické bezpečnosti v příloze č. 8.

3. Tato Smlouva se vyhotovuje ve 2 (slovy: dvou) stejnopisech, z nichž každá ze Smluvních stran obdrží po 1 (slovy: jednom) vyhotovení, přičemž každý stejnopis má platnost originálu. V případě jakéhokoliv rozporu mezi českou a anglickou verzí této Smlouvy, je rozhodující česká verze.

4. Smluvní strany berou na vědomí a souhlasí s tím, že Objednatel uveřejní metadata k této smlouvě a textový obsah smlouvy v informačním systému registru smluv zřízeném podle zákona 340/2015 Sb. ve znění pozdějších předpisů bez zbytečného odkladu po podpisu smlouvy.

5. Tato Smlouva a právní vztahy z této Smlouvy vyplývající se řídí právním řádem České republiky, zejména Občanským zákoníkem. K řešení případných sporů vzniklých z této Smlouvy jsou příslušné soudy České republiky.

6. Tato Smlouva může být měněna pouze dohodou Smluvních stran, a to formou písemných vzestupně číslovaných dodatků podepsaných oběma Smluvními stranami.

7. Smluvní strany prohlašují, že se považují za rovnocenné smluvní partnery a žádná z nich se nepovažuje za slabší Smluvní stranu.

8. Smluvní strany prohlašují, že by k uzavření této Smlouvy došlo i tehdy, kdyby kterákoli její část byla neplatná nebo se neplatnou stala dodatečně a pro tyto případy považují tuto Smlouvu jako celek za platnou s tím, že neplatné ustanovení se nahradí jiným ustanovením, které nejlépe odpovídá obsahu a účelu neplatného ustanovení. Smluvní strany se vzájemně zavazují, že budou spolupracovat při tvorbě takového ustanovení.

9. Smluvní strany na sebe berou nebezpečí změny okolností a nemůžou se tedy domáhat jakýchkoliv práv na základě jakékoliv změny takových okolností.

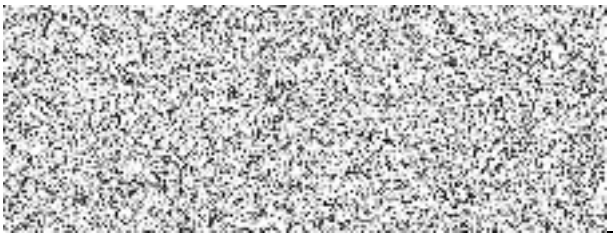
10. Smluvní strany potvrzují, že si tuto Smlouvu před jejím podpisem přečetly, porozuměly jejímu obsahu, že vyjadřuje jejich pravou, vážnou a svobodnou vůli, na jejich straně nejsou žádné překážky, které by bránily sjednání a podpisu této Smlouvy, a uzavírají ji svobodně za vzájemně výhodných podmínek. Na důkaz toho připojují své níže uvedené podpisy.

XIV. **Přílohy**

4188656-Příloha 1 ZD - Krycí list nabídky
4268543-Příloha 5 ZD - Podrobná specifikace předmětu plnění a požadavky na realizaci zakázky, část tech. kvalifikace_3v0
Příloha č.3 - Čestné prohlášení o opatřeních k mezinárodním sankcím

V …… dne ……

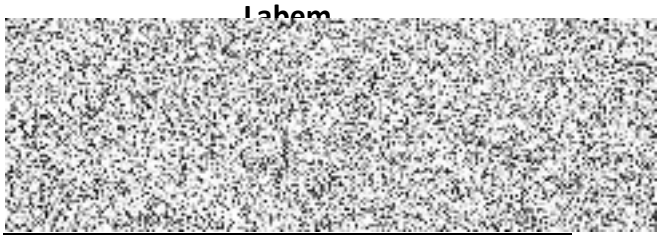
Mepatek s.r.o.



Daniela Dohnalová,
Jednatel společnosti

V …… dne ……

Zdravotní ústav se sídlem v Ústí nad Labem



Ing. Eduard Ježo
Ředitel

Krycí list nabídky

k veřejné zakázce

Veřejná zakázka: **ZUUL – Zvýšení kybernetické bezpečnosti**

Zadavatel: **Zdravotní ústav se sídlem v Ústí nad Labem**
Moskevská 1531/15, 400 01 Ústí nad Labem
IČ71009361

1. Identifikační a kontaktní údaje účastníka		
Obchodní jméno účastníka		**Mepatek s.r.o.**
Sídlo / místo podnikání		Teplická 305, 417 61 Bystřany
Oprávněná osoba (*jméno a příjmení statutárního orgánu nebo jeho členů, případně jiné osoby oprávněné zastupovat účastníka v předmětném zadávacím řízení)*		Daniela Dohnalová, jednatelka společnosti
IČ		27268080
DIČ		CZ27268080
Doručovací adresa, vč. PSČ		Teplická 305, 417 61 Bystřany
Kontaktní údaje v otázkách plnění zakázky	Telefon	[redacted]
	e-mail	[redacted]
2. Výše celkové nabídkové ceny za veškerá plnění v zakázce (poskytnuté dodávky a implementace technologií podle podmínek uvedených v zadávací dokumentaci a jejích přílohách)		
Část veřejné zakázky, do které je nabídka podávána (doplnit číslo a název části)		**Část 01 - Komodity K.1 a K.2 - Zvýšení zabezpečení komunikační sítě, nástroje pro zajišťování úrovně dostupnosti informací.**
Celková nabídková cena v Kč bez DPH		**8 170 004**
DPH		1 715 700,84
Celková nabídková cena v Kč s DPH		9 885 704,84

V Bystřanech dne 20.5.2024

Daniela Dohnalová, jednatelka společnosti

Podrobná specifikace předmětu plnění a požadavky na realizaci zakázky, části technické kvalifikace

1. Podrobný popis předmětu plnění

(1) Předmětem plnění veřejné zakázky je dodávka a implementace technologií pro zvýšení kybernetické bezpečnosti informačních systémů (IS) a komunikačních systémů (KS) zadavatele v souladu se standardy kybernetické bezpečnosti (dále také jen „dodávka“, „systém“, „řešení“ nebo „technologie“), včetně nezbytných služeb. Podrobná specifikace dodávek a služeb je uvedena v dalších kapitolách tohoto dokumentu. Součástí plnění je dále zajištění provozu (maintenance) na dobu minimálně 60 měsíců po předání řešení do ostrého provozu. Řešení musí být navrženo tak, aby náklady na provoz systémů byly co nejmenší.

(2) U technických parametrů, u kterých není výslovně uvedeno, že jde o požadovanou minimální či maximální hodnotu, lze nabídnout i řešení „lepší“, tedy řešení přesahující (ve smyslu výhodnějším z pohledu užitné hodnoty) hodnotu stanoveného požadavku, ledaže ze zadávacích podmínek výslovně vyplývá, že musí být splněna přesně daná hodnota.

(3) Veřejná zakázka je rozdělena na tři části, jak je uvedeno i v článku 3.2.2. zadávací dokumentace.

Část 01	Komodity K.1 a K.2 - Zvýšení zabezpečení komunikační sítě, nástroje pro zajišťování úrovně dostupnosti informací.
Část 02	Komodita K.3 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému.
Část 03	Komodita K.4 - Ochrana EDR/XDR.

(4) Předmětem plnění veřejné zakázky jsou zařízení a systémy uvedené v následující tabulce, včetně služeb (komodity):

Komodita	Zajišťovaná oblast	Stručný popis položky	Jednotka	Počet jednotek
K.1	Zvýšení zabezpečení komunikační sítě	1. Zavedení řízení přístupu do sítě podle standardu IEEE 802.1X. 2. Provedení plné segmentace sítě ZUUL včetně výměny aktivních prvků. Součástí je dodávka software pro řízení přístupu k fyzickým i bezdrátovým sítím na bázi protokolu IEEE 802.1X, dodávka aktivních prvků, implementace a související služby.	soubor	1
K.2	Nástroje pro zajišťování úrovně dostupnosti informací	1. Nástroj pro zajištění úrovně dostupnosti záloh ZUUL 2. Zálohovací server 3. Diskové úložiště 4. Dva nové servery 5. UPS	Soubor	1

Komodita	Zajišťovaná oblast	Stručný popis položky	Jednotka	Počet jednotek
		Součástí je pořízení zálohovacího serveru, diskového úložiště, hypervisorů, UPS a serveru nebo hardwarové appliance pro bezpečné ukládání záloh a jejich ochranu proti poškození a související služby.		
K.3	Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů (Log/Event Management) Zavedení nástroje pro auditování Active Directory	1. Zaznamenávání činností (logů) z datových center, virtuálních serverů, firewallů, switchů atd. a souvisejících systémů do externích systémů. 2. Nástroje pro kompletní správu životního cyklu (pořízení, zpracování, zobrazení, prohledávání, ochrana, uchování a archivace) logů chráněných IS a souvisejících a podpůrných systémů a technologií. 3. Pokročilé notifikační nástroje bezpečnostních a nestandardních událostí. 4. Implementace pro auditování činností uživatelů a administrátorů, auditování Active Directory. Součástí je pořízení software pro komplexní správu logů (log management), hardware nebo hardwarové appliance pro běh software, implementace a související služby. Dále pak nasazení nástroje auditování činností uživatelů a administrátorů.	soubor	1
K.4	Ochrana typu Endpoint Detection and Response (EDR) nebo Rozšířené detekce a reakce (XDR)	1. Nástroj pro zajištění ochrany serverů a koncových zařízení. Součástí je pořízení nástroje sloužícího k identifikaci persistentních hrozeb a cílených útoků, snížení reakční doby na incident a k proaktivní preventivní ochraně proti útokům.	Soubor	1

2. Požadované parametry technického řešení

2.1. Obecné požadavky

(1) Zadavatel při výstavbě, správě a provozu technologií striktně dodržuje hledisko technologické neutrálnosti, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců – tuto strategii musí splňovat i řešení dodané v rámci této veřejné zakázky.

(2) Pokud uchazeč vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

(3) Za předpokladu, že uchazečem navržené řešení vyžaduje fyzickou infrastrukturu (např. servery, úložiště, komunikační prvky atd.) neobsaženou v popisu předmětu plnění, zahrne uchazeč do své ceny všechny náklady na její pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.

(4) Pro každý softwarový produkt, který uchazeč nabídne v rámci svého řešení, budou v nabídce výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně uvedení konkrétní infrastruktury, na které bude řešení provozováno.

(5) Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že uchazeč vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky – není přípustné implementovat např. další serverovou virtualizační platformu, adresářovou službu apod.

(6) Uchazeč prokáže, že všechny dodávky, které dodá Zadavateli:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,

(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,

(d) obsahuji licenci na používání příslušného softwaru,

(e) jsou určeny pro provoz v České republice,

(f) z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

Tyto skutečnosti uchazeč doloží čestným prohlášením distributora, popř. uchazečem samotným, nelze-li prohlášení distributora získat. Zadavatel si vyhrazuje právo na zjištění původu výrobku při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

2.2. Specifické požadavky – K1 – Zvýšení zabezpečení komunikační sítě ZUUL

(1) Komunikační síť ZUUL lze rozčlenit na 2 logické části – LAN centrálního datového centra UnL a Kladno, VPN jednotlivých poboček. LAN je prostřednictvím firewallů dále propojena s dalšími veřejnými sítěmi (internet). Pobočky jsou prostřednictvím VPN připojeny pouze do LAN, s jinými sítěmi mohou komunikovat pouze jejím prostřednictvím. Pobočky i centrála jsou vybaveny Wi-Fi přístupovými body. Segmentace sítě (VLAN) je jen základní, zařazování zařízení do VLAN je statické. Zařízení není při připojení do sítě identifikováno a má přístup do sítě odpovídající nastavení portu přepínače, do kterého se zařízení zapojí.

(2) Zvýšení bezpečnosti komunikační sítě bude dosaženo implementací:

(a) granulární a dynamické segmentace sítě s využitím protokolu IEEE 802.1X – zařízení bude při připojení do sítě ověřeno a podle své charakteristiky (a uživatele) mu bude na základě politik umožněn přístup do sítě a bude zařazeno do odpovídající VLAN bez ohledu na místo/způsob připojení.

(3) V rámci plnění tedy bude v celé LAN implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby Active Directory s využitím technologie 802.1X.

(4) Dále bude implementován systém centrální správy, který poskytne celkový pohled na stav a konfiguraci LAN jako celku a současně umožní centrálně provádět změny konfigurace prvků LAN a vytvořením jednotně spravovaných VLAN zavést segmentaci sítě. Součástí centrálního systému bude systém řízení přístupu zařízení a uživatelů do síťové infrastruktury založený na standardu IEEE 802.1X a systém ověření původu DNS záznamů elektronickým podpisem.

(5) Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN. Součástí dodávky je vzorová konfigurace 802.1X na všech typech uživatelských koncových zařízení Objednatele (PC, notebooky, chytré telefony, tablety, tiskárny – Windows, Linux, MacOS, Android, IOS, embedded systémy periferií) a uživatelská dokumentace pro konfiguraci koncových zařízení uživateli.

(6) Systém musí umožňovat v budoucnu i ověřování přístupu do Wi-Fi sítě, které bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wi-fi bude nabízet více SSID (např. zaměstnanci, hosté, IoT) které budou obsluhovány samostatnými VLAN a budou napojeny na radius

servery. Zaměstnanci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) bude provedeno s využitím WPA3 (alternativně WPA2 dle podpory připojovaných zařízení) s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Řešení umožní použití autentizace prostřednictvím webového portálu (tzv. captive portál) s využitím jednorázových přístupových údajů a samostatných politik a restrikcí pro tento způsob autentizace.

(7) Pro Wi-Fi budou zřízeny samostatné VLAN, které budou komunikačně odděleny od ostatních vnitřních sítí organizace. Tyto VLAN budou konfigurovány na úrovní stávajícího firewallu tak, aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a bude jim být přiřazen samostatný profil a/nebo virtuální kontext nakonfigurovaný ve firewallu.

(8) Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s přepínáním provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.

(9) Součástí plnění je implementace pořízených technologií včetně osazení aktivních síťových prvků (přepínače) v centrále i na pobočkách v Ústeckém kraji do připravených racků a na připravenou kabeláž (pasivní část LAN není součástí tohoto projektu).

Typ přepínače	**Konfigurace switche**
A	Datacenterový přepínač 24p 10Gbe SFP+, 4 porty 56Gbe
B	Klientský přepínač typ 24 portů, 4 SFP+ 10Gbe
C	Klientský přepínač typ 24 portů, 4 SFP+ 10Gbe, PoE
D	Klientský přepínač typ 48 portů, 4 SFP+ 10Gbe
E	Klientský přepínač typ 48 portů 4 SFP+ 10Gbe, PoE
F	Klientský přepínač typ 12 portů 2 SFP+ 10Gbe, PoE

2.3. Specifické požadavky – K2 – Nástroje pro zajišťování úrovně dostupnosti informací

Pro provoz aplikací a systémů využívá ZUUL virtualizační platformu založenou na Hyper-V a sestavenou ze 2 fyzických serverů v lokalitě Ústí nad Labem a Kladno (celkem 4 servery, hypervisory). V případě lokality Kladno je disková kapacita platformy tvořena interními disky serverů. V lokalitě Ústí n/L je k dispozici diskové pole, jehož kapacita ani výkon není dostatečný a infrastruktura tak není schopna zajistit dostatečnou dostupnost výpočetních zdrojů hostovaným aplikacím a systémům. Servery v lokalitě UnL nemají dostatek RAM a v případě výpadku jednoho z nich nebo při plánované údržbě není možné provoz přesunout na stávající server. Současně nejsou HW kapacity dostatečné pro provoz nově pořizovaných nástrojů.

(1) Zálohování ZUUL je prováděno automaticky pokročilým zálohovacím systémem Veeam Backup & Recovery v edici Standard v lokalitě Ústí n/L a v edici Enterprise v lokalitě Kladno.

Zálohovací systém v lokalitě DC Ústí n/L zálohy plně kontroluje, tj. při jeho kompromitaci či poškození může dojít k znepřístupnění záloh.

(2) Zvýšení úrovně dostupnosti informací bude dosaženo:

(a) Pořízením nového diskového pole s dostatečným výkonem i kapacitou do lokality DC Ústí n/L. kompatibilní se s nově dodávanými hypervisory. Diskové pole bude připojené redundantně k nově dodávaným datacenterovým přepínačům.

(b) Nákup dvou nových serverů, hypervisorů s dostatečným výkonem pro zajištění dostupnosti informací pro stávající i nově pořizované bezpečnostní systémy. Servery budou připojeny redundantně k nově dodávaným datacenterovým přepínačům.

(c) Implementací bezpečného datového úložiště pro zálohy – požadováno je zařízení s nastavitelnou retencí ukládaných dat (záloh) tak, aby uložená data nebylo možné po určitou (nastavitelnou) dobu změnit. Z pohledu zálohovacího systému půjde o zařízení typu WORM (Write One, Read Many) do lokality DC Ústí n/L

(d) Pořízením samostatného zálohovacího serveru, který bude provozován nezávisle na virtualizované infrastruktuře, čímž dojde ke zvýšení bezpečnosti provozu zálohovacího severu a nárůstu kapacity celého zálohovacího řešení pro ukládání záloh, aby odpovídala nárůstu požadavků na rozšíření datové kapacity serverů

(e) Pořízením dostatečně dimenzovaného zdroje nepřerušitelného napájení s dostačenou kapacitou a dobou provozu v případě výpadku el. Energie, čímž dojde k celkovému zvýšení spolehlivosti provozu a dostupnosti dat.

(3) V rámci komodity bude vybudováno bezpečné úložiště pro ukládání dat, která musí být ochráněna proti jakékoli modifikaci po určenou dobu (retenční lhůtu). Jedná se např. o zálohy databází, kritická nestrukturovaná data, ale kompletní zálohy virtuální serverů apod. Úložiště umožní konfigurovat více kategorií chráněných dat a odpovídajících retenčních lhůt. Data bude možné ukládat pomocí běžných síťových protokolů, např. SMB/CIFS.

(4) Úložiště bude nativně spolupracovat se stávajícím zálohovacím systém pro možnost přímého ukládání záloh kritických dat a jejich ochrany před zničením škodlivým kódem (např. ransomware) nebo jiným způsobem.

2.4. Specifické požadavky – K3 – Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů (Log/Event Management)

(1) V současné době nevlastní ZUUL žádný nástroj pro (centrální) zaznamenávání činnosti (logů) a navazujících systémů. Činnosti jsou v některých systémech zaznamenávány lokálně, ale bez jednotné politiky, dlouhodobého ukládání a ochrany logů před změnou, přetečením apod. Chybí tak nástroj pro podporu řešení případných kybernetických událostí a incidentů, poskytování konsolidovaných informací před vznikem a v průběhu události/incidentu. Absence nástroje také neumožňuje efektivně analyzoval chování IS a souvisejících systémů z pohledu kybernetické bezpečnosti, ale i z pohledu běžného provozu pro účely zavádění preventivních opatření předcházejících výskytu nestandardního provozního stavu a/nebo opatření k zamezení jeho opakování.

ZUUL v současnosti nevlastní žádný nástroj, který by poskytoval úplný přehled o tom, co se děje ve službě Active Directory a zásadách skupin, ani nástroj, který by poskytoval bezpečnostní analýzy, které by pomohly odhalit anomálie chování uživatelů, identifikovat potenciální vnitřní hrozby, efektivně vyšetřovat a hlásit bezpečnostní incidenty dříve, než dojde k narušení. Nelze tedy provádět ani audity Active Directory.

(2) Zvýšení úrovně zabezpečení v oblasti řízení přístupových oprávnění interních i externích správců bude dosaženo:

(a) Implementací nástroje pro správu logů (tzv. log management) - zavedením komplexního systému pro správu logů dojde ke centralizovanému sjednocení různých bází bezpečnostních a provozních záznamů, které jsou poskytovány různými typy hardwarových zařízení, dále různými provozovanými operačními systémy a aplikacemi, včetně všech nástrojů implementovaných v rámci tohoto projektu. Zaznamenané činnosti budou k dispozici na jednom místě ve sjednoceném formátu při zachování jejich dostupnosti, důvěrnosti a integrity. Systém zajistí uložení dat k okamžitému prohlížení a prohledávání minimálně po dobu 6 měsíců a bude umožňovat archivaci starších záznamů s možností rychlé obnovy archivu v případě potřeby. Systém musí zajistit integritu archivu.

(b) Pořízením vyhrazeného serveru nebo hardwarové appliance pro provoz nástroje pro správu logů, aby byla zajištěna nezávislost nástroje na infrastruktuře ZUUL a tím schopnost zaznamenávání její činnosti i v nestandardních provozních stavech (přetížení, start, nestabilita apod.), bezpečnost proti Ransomware a potřeba velkého výpočetního výkonu.

(c) Implementací nástroje pro auditování Active Directory, který bude poskytovat přehled o všech změnách zabezpečení a konfigurace v Active Directory, zásadách skupin, eskalaci oprávnění, anomální aktivitách správců, podezřelé pokusy zaměstnanců a další.

(3) Požadované řešení je standardní Log/Event Management s možností rozšíření na SIEM nebo musí umožnit budoucí rozšíření o další systémy (např. systém SIEM) nebo napojení na služby SOC (Security operations center).

(4) Řešení umožní sofistikovanou, transparentní a opakovatelnou pokročilou analýzu, spojenou s řešením běžných provozních i bezpečnostních událostí/incidentů a upozorňováním na ně, a to z kritických i nekritických a podpůrných systémů a aplikací. Řešení musí být schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, primárně v českém jazyce a dále variantně v jazyce anglickém, bez nutnosti používat SQL (či obdobnou „programátorskou“) syntaxi pro definici či úpravu reportů.

(5) Nabízené řešení musí zachovávat originál logů za účelem bezpečnostního auditu, a to v souladu s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů.

(6) Řešení musí umožnit snadné a rychlé multikriteriální vyhledávání pro účely analýz, auditů, a podporu běžného provozu komplexního řešení ICT infrastruktury ZUUL.

(7) Pro zajištění požadavků bezpečnosti musí řešení Log/Event Management disponovat konfigurovatelným uživatelským oddělením rolí a ochranou centralizovaných logů před neoprávněným přístupem k citlivým datům.

(8) Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly") organizace.

(9) Data uložená v systému a systémem archivovaná budou zajištěna a zabezpečena před neoprávněnou změnou i pro účely vyšetřování případného bezpečnostního incidentu.

(10) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o HW (fyzický server včetně nainstalovaného licencovaného OS) + nainstalovaný softwarový nástroj nebo appliance. Zařízení umožní správu z jedné grafické konzole přístupné nativně skrze https. Ukládání všech informací do bude prováděno jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých.

(11) Mandatorní informace, která bude v systému vždy obsažena a uchována je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích na straně firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (např. RADIUS logy). Dále budou získávány informace o překladu zdrojových, vnitřních IPv4 adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.

(12) Bude umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopný dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat, resp. reportovat.

(13) Implementace systému bude v provedena v souladu s § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí Vyhlášky č.316/2014 Sb. k Zákonu č. 181/2014 Sb., o kybernetické bezpečnosti.

(14) Zadavatel může uchazeče vyzvat k doručení funkčního vzorku. Pokud zadavatel vyzve uchazeče o poskytnutí funkčního vzorku (v identické konfiguraci s nabízeným systémem) pro účely testování a ověření požadovaných funkčních vlastností, uchazeč je povinen doručit testovací vzorky na Místo plnění do pěti (5) pracovních dnů od doručení výzvy k jejich poskytnutí. Vybraný uchazeč poskytne testovací vzorky bezplatně a na dobu minimálně následujících 10 pracovních dnů poskytne i součinnost s testováním.

(15) Požadované řešení pro zajištění auditování Active Directory musí umožňovat získat přehled o tom co se děje v Active Directory, zásadách skupiny apod., poskytovat bezpečnostní analýzy, které pomohou odhalit neobvyklé chování uživatelů. Identifikovat potencionální vnitřní hrozby, každou takovou hrozbu klasifikovat atd. Nevyžaduje se tzv. agentless architektura (může být i agentová architektura), která nesnižuje výkon systému s Restful API, kterou je možné integrovat např. s aplikacemi třetích stran.

(16) Bude upozorňovat na kritické události zabezpečení Active Directory, jakmile k nim dojde, podezřelé pokusy o přihlášení, nepřetržité hlášení o úspěšných i neúspěšných přihlášeních ve službě Active Directory, zprávy o konfiguraci Active Directory, možností vyhledávání (podobné vyhledávání google) k urychlení vyhledávání při vyšetřování bezpečnostních incidentů, které bude umožňovat zadání jedinečných vyhledávacích kritérií.

(17) Dále bude řešení disponovat předdefinovanými sestavy s řídícími panely informující o všech změnách uživatelů, skupin, organizačních jednotek, řadičů domény a dalších objektů, vlastností, nastavení a oprávnění. Součástí řešení bude i funkce upozornění na vypršení platnosti hesla či možnost sledování neaktivních uživatelů/účtů.

(18) Řešení bude umožnovat průběžnou kontrolu změn provedených privilegovanými uživateli v Active Directory s možností automatické notifikace s podrobnostmi o každé změně provedené v konfiguracích AD. V oznámeních budou uvedeny změny objektů AD, nově vytvořené a odstraněné objety GPO, změny propojení objektů GPO, změny provedené v zásadách auditu, zásadách hesel, nasazení software atd.

(19) Řešení bude detekovat bezpečností rizika Active Directory, klasifikovat je a definovat úrovně rizik např. v rozsahu nízké, střední, vysoké.

2.5. Specifické požadavky – K4 – Ochrana typu Endpoint Detection and Response (EDR) nebo rozšířené detekce a reakce (XDR)

(1) Implementací se rozumí zprovoznění konzole (případně dalších potřebných komponent) v prostředí Hyper-V a řešení EDR/XDR na všech koncových stanicích ZUUL.

(2) Konzultace a návrh konkrétní implementace – dodání dokumentací a nutných technologických požadavků pro správný návrh a funkčnost řešení.

(3) Nastavení vzorové bezpečnostní politiky a karantény – min. v rozsahu dle tzv. best practices výrobce a dle projektové dokumentace

(4) Implementace včetně odpovídajícího zaškolení odpovědných osob na straně objednatele

(5) Předání veškeré související dokumentace

(6) Řešení EDR/XDR má centrální správu v cloudu, připouští se umístění pouze v EU.

(7) Součástí EDR/XDR systému je také endpoint antivirus.

2.6. Specifické požadavky – povinné parametry řešení

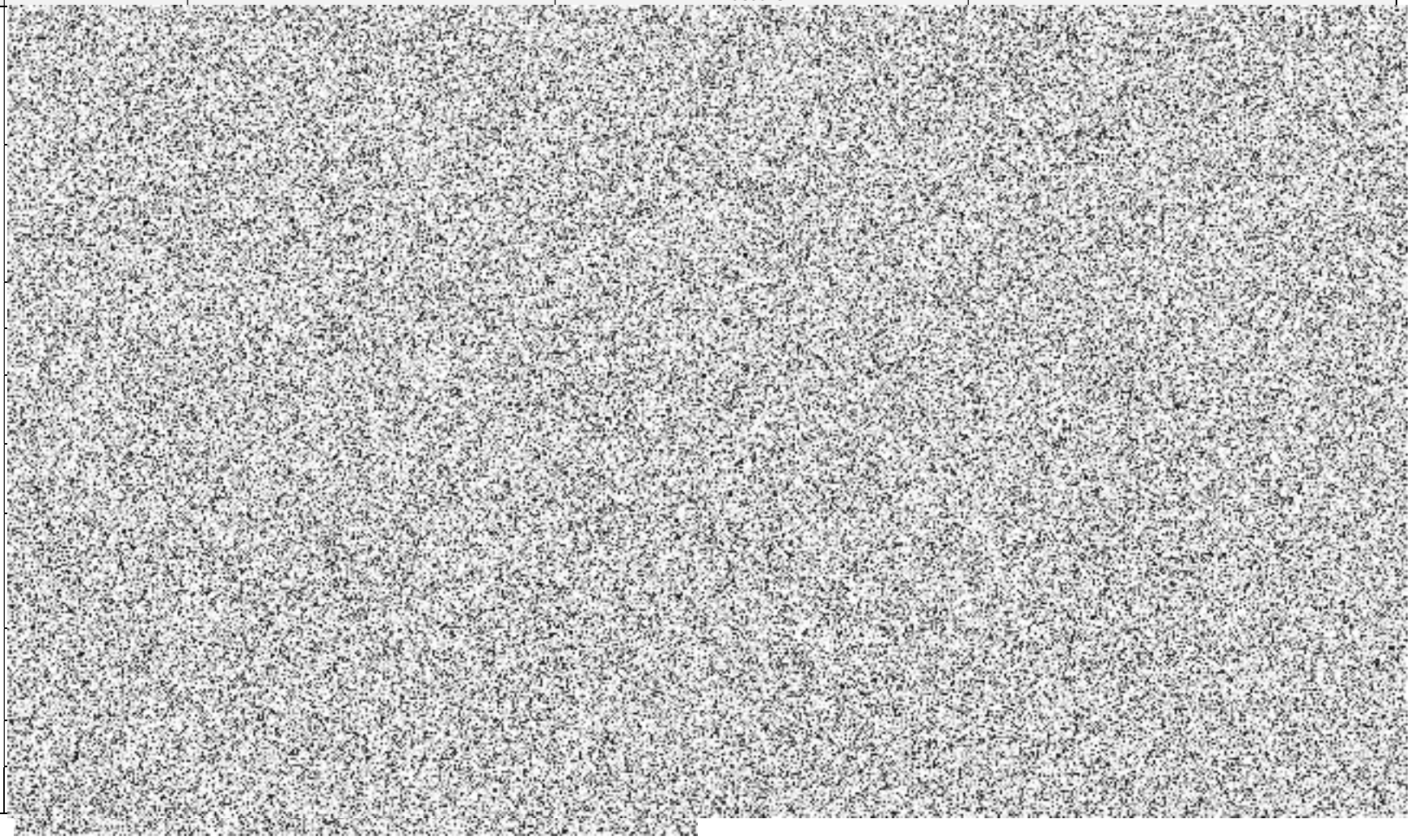
(1) V dále uvedených tabulkách jsou uvedeny minimální požadované (povinné) parametry dodávaného řešení.

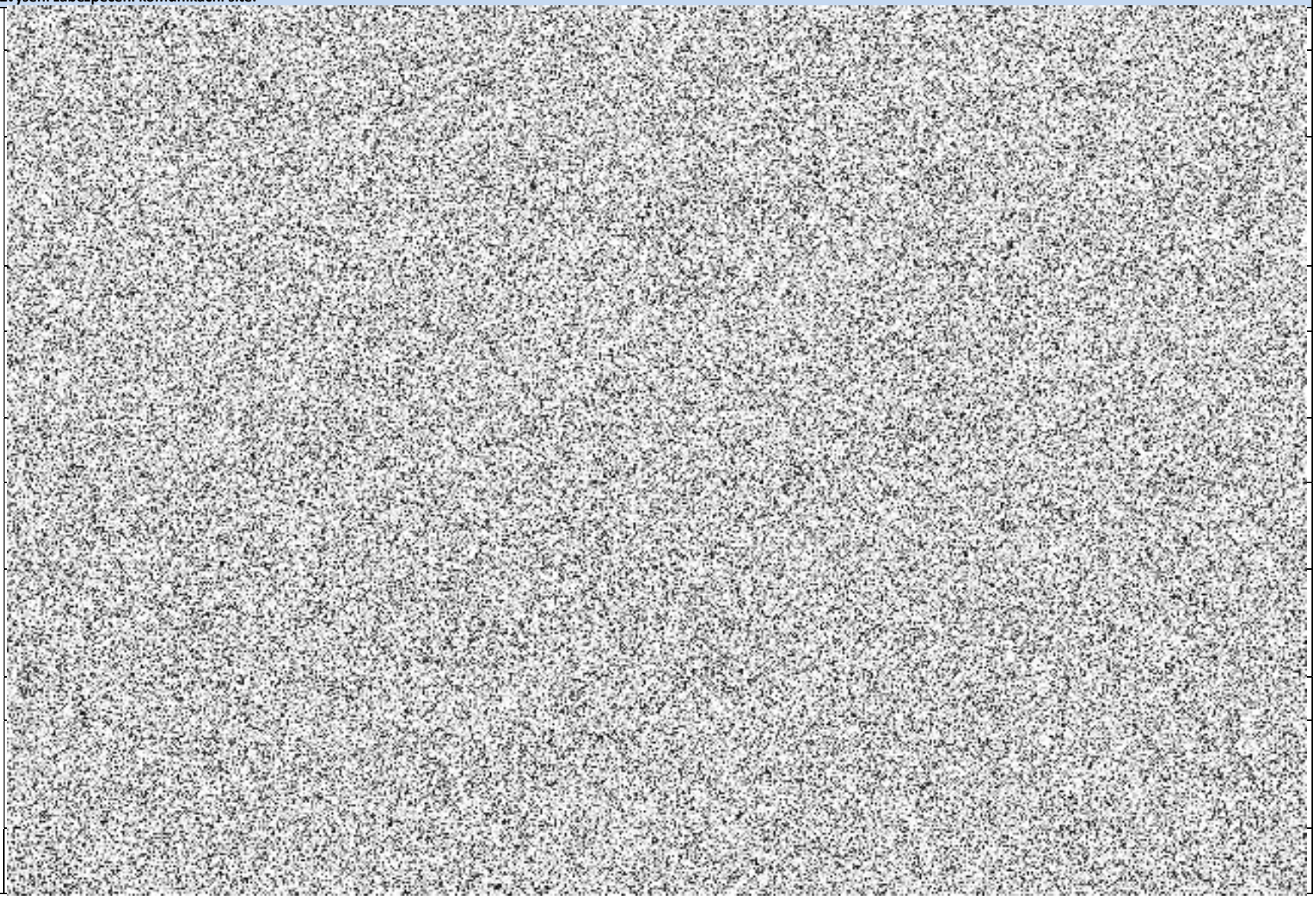
(2) **Účastník ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Účastník tedy uvede konkrétní technické parametry nabízeného zboží, vč. uvedení výrobce a obchodního / typového označení jednotlivých komponentů. Údaje o výrobci a obchodním (či typovém) označení budou uvedeny a doloženy v tabulkách povinných parametrů; konkrétní parametry mohou být buď rovněž doplněny do tabulky, nebo mohou být doloženy jinde v nabídce např. formou katalogových listů apod., v takovém případě ale musí být v tabulce odkázáno na část nabídky, ve které je možné naplnění parametru ověřit.**

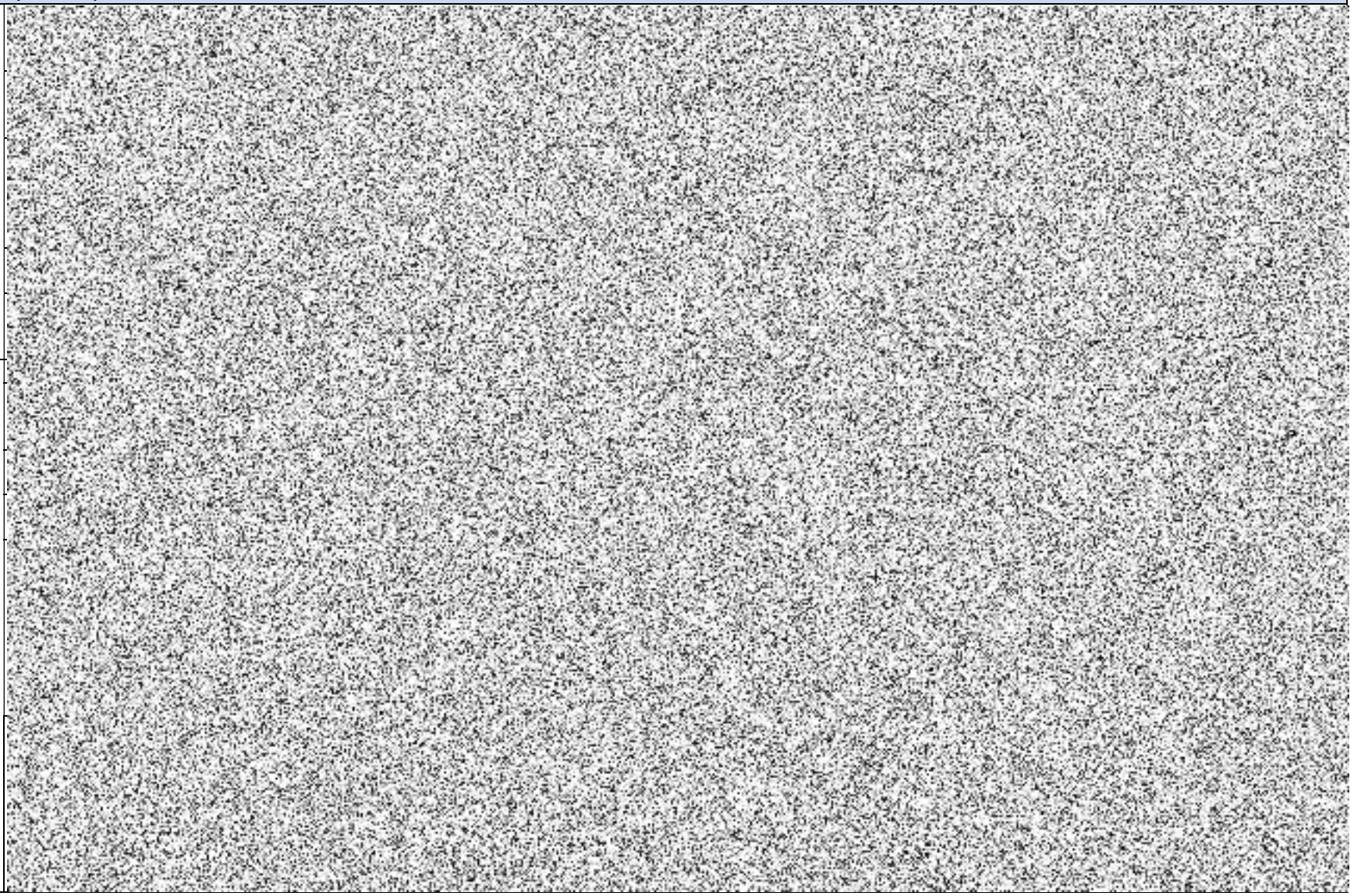
(3) **Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí prokazovat (nepostačuje pouze potvrzení či zkopírování požadavku Zadavatele), že nabízené řešení jednoznačně splňuje všechny požadavky.**

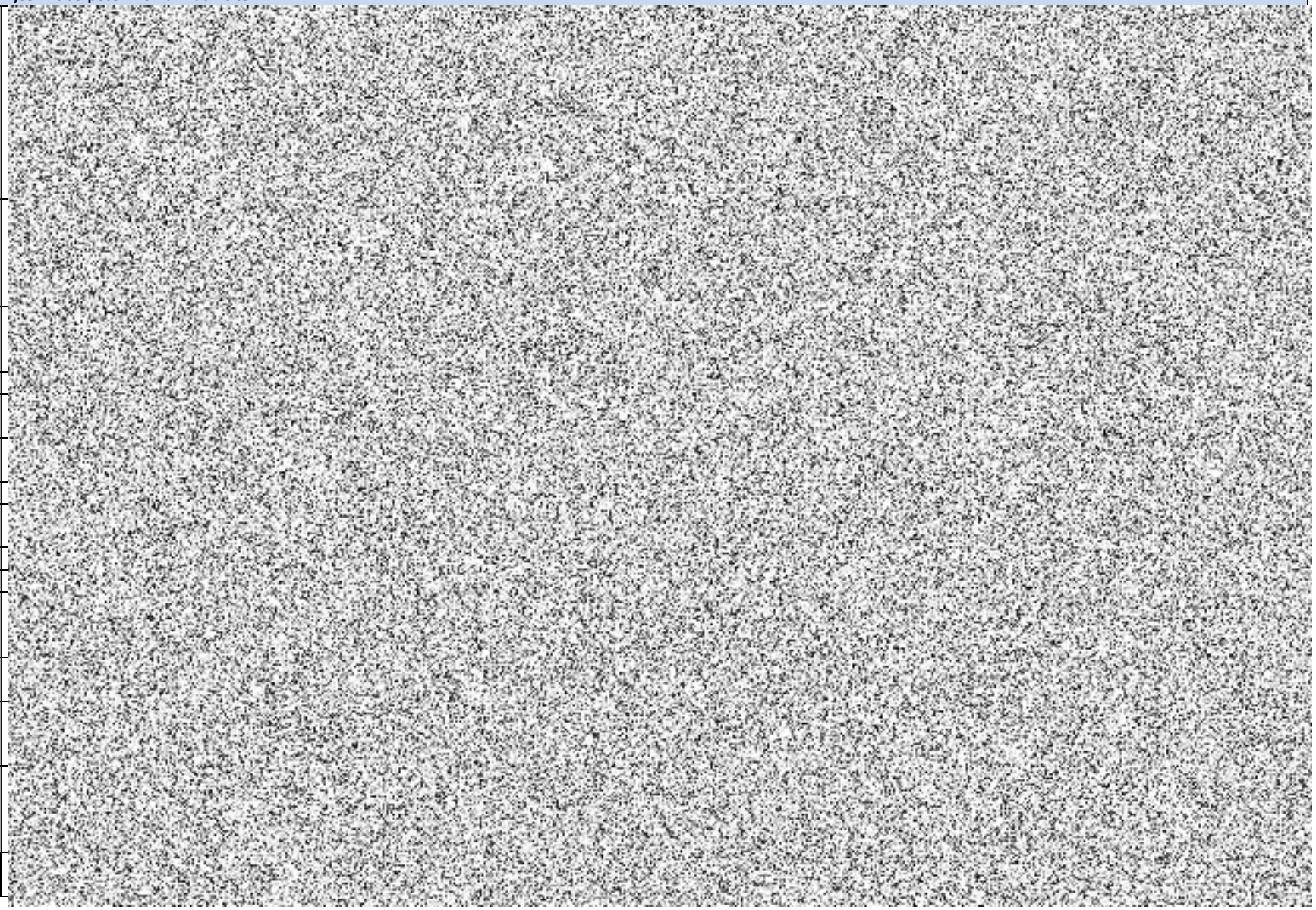
(4) **Uchazeč musí všechny povinné parametry splnit, v případě nesplnění je jeho nabídka vyloučena.**

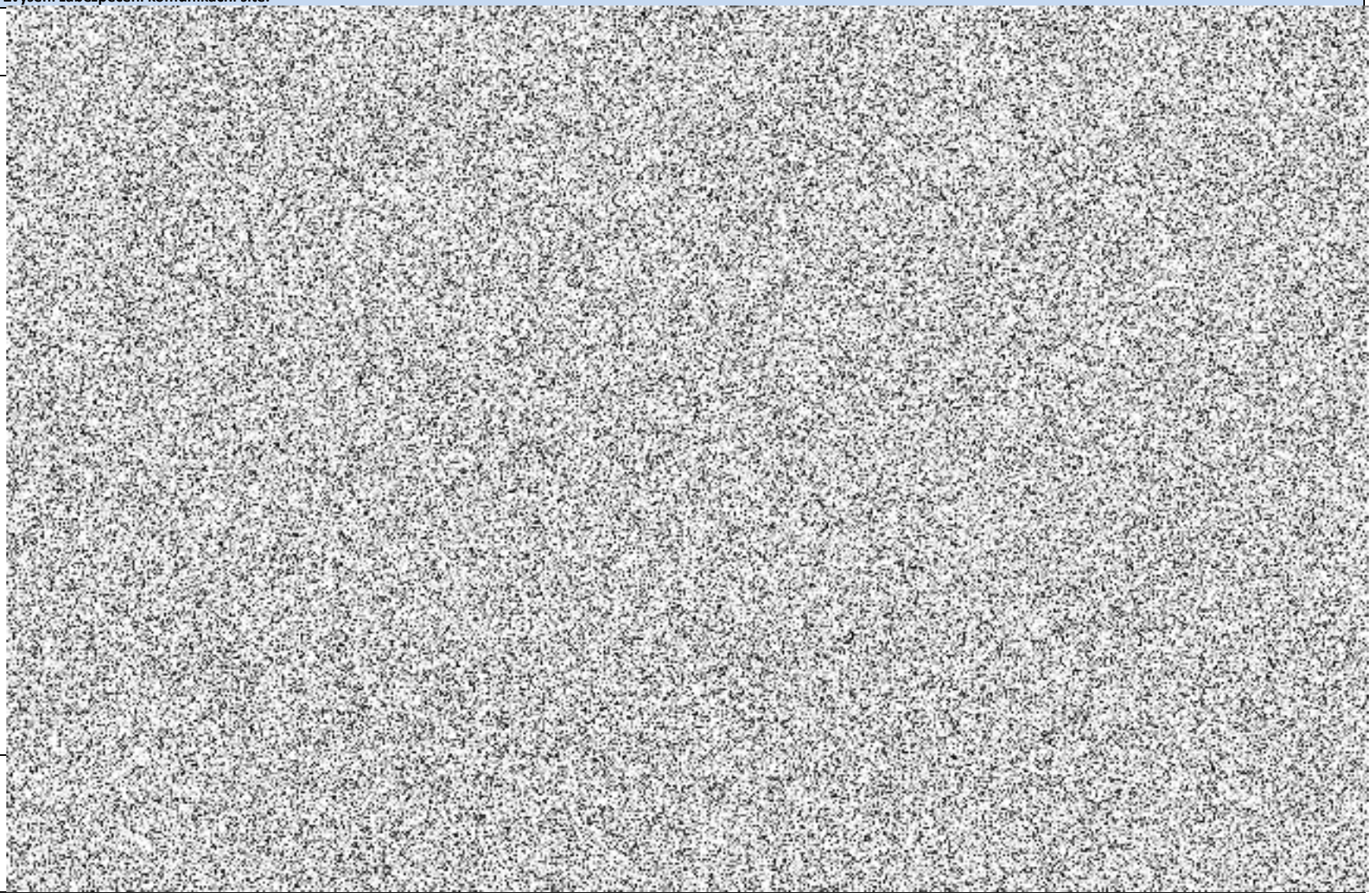
(5) Požadavky na zvýšení zabezpečení komunikační sítě:

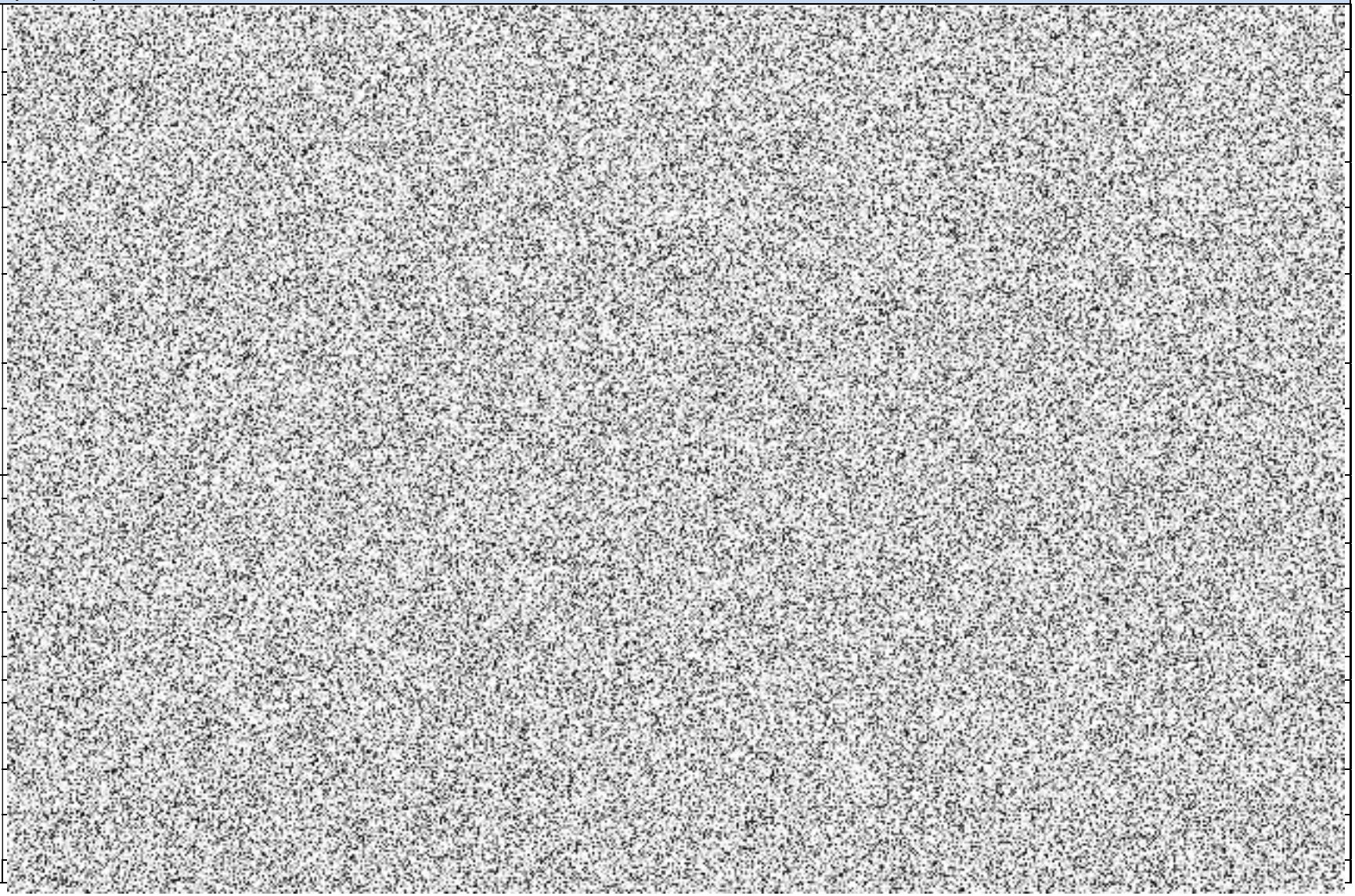
Komodita K.1 - Zvýšení zabezpečení komunikační sítě.				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Systém řízení přístupu do sítě podle standardu IEEE 802.1X				

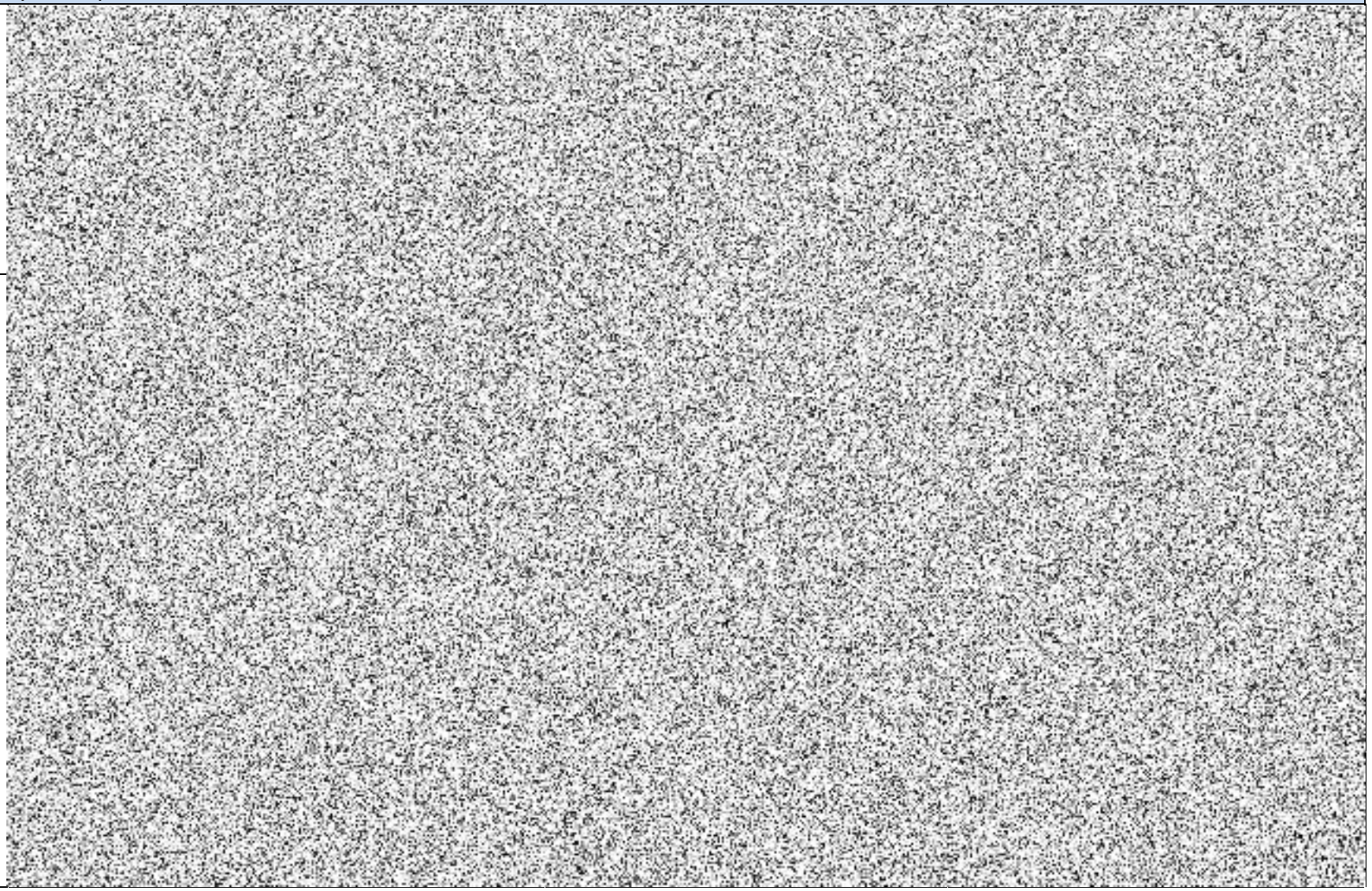
Komodita K.1 - Zvýšení zabezpečení komunikační sítě.	
	

Komodita K.1 - Zvýšení zabezpečení komunikační sítě.	
	
Centrální přepínač typ A 2x	

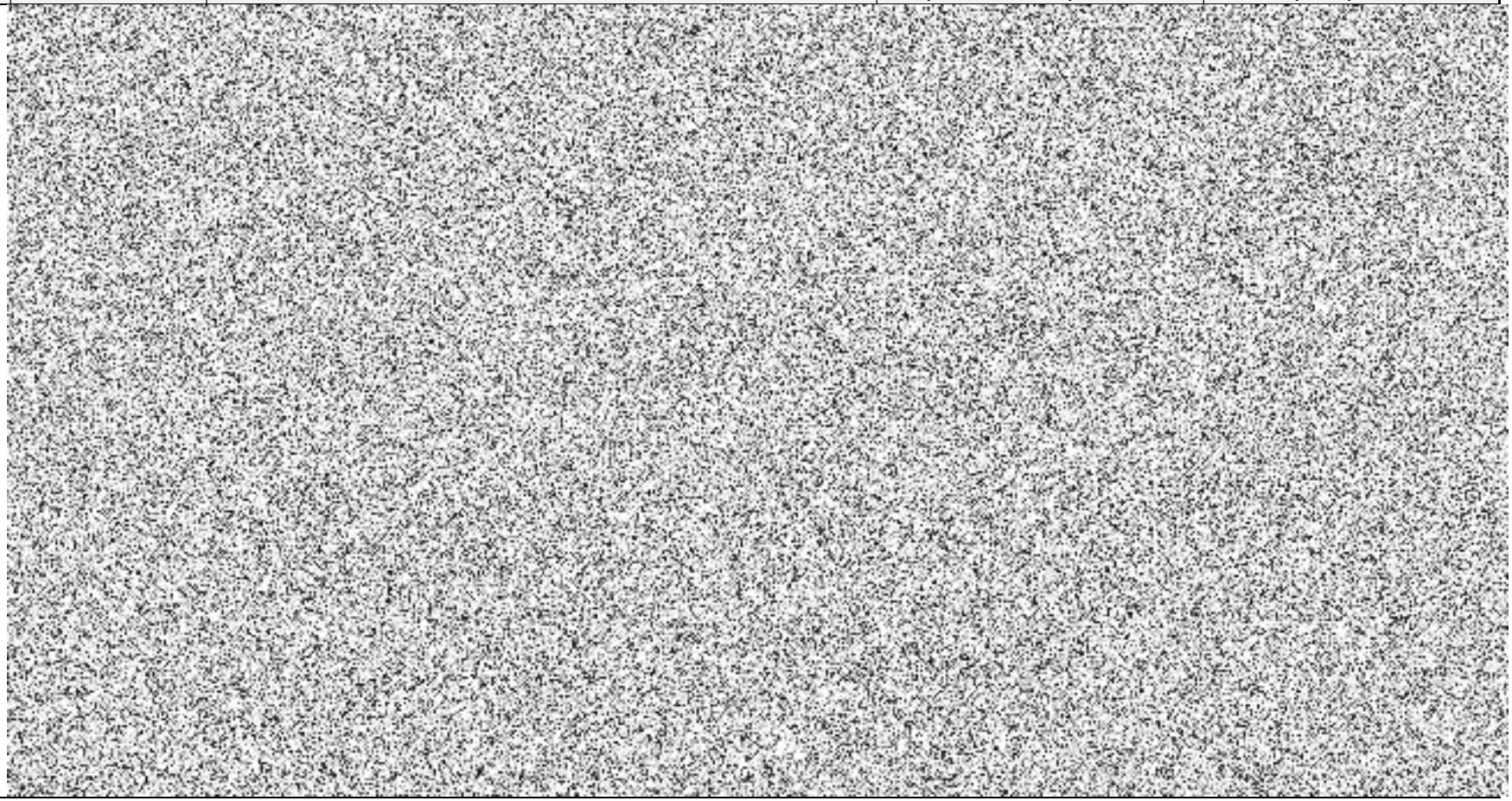
Komodita K.1 - Zvýšení zabezpečení komunikační sítě.	
	
Přístupový přepínač typ B 10x	

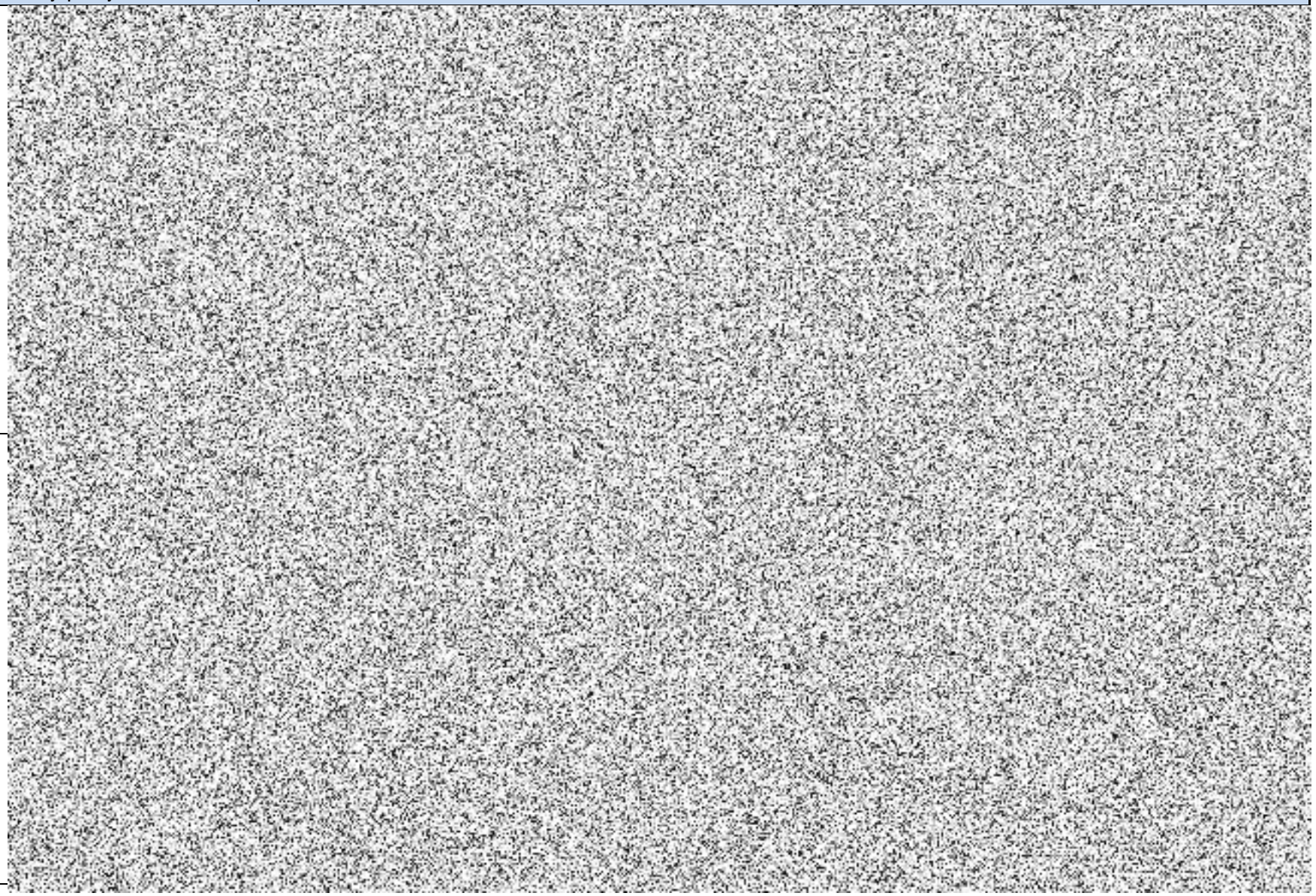
Komodita K.1 - Zvýšení zabezpečení komunikační sítě.	
	
Přístupový přepínač typ C 12x	
Přístupový přepínač typ D 2x	

Komodita K.1 - Zvýšení zabezpečení komunikační sítě.	
	
Přístupový přepínač typ E 8x	

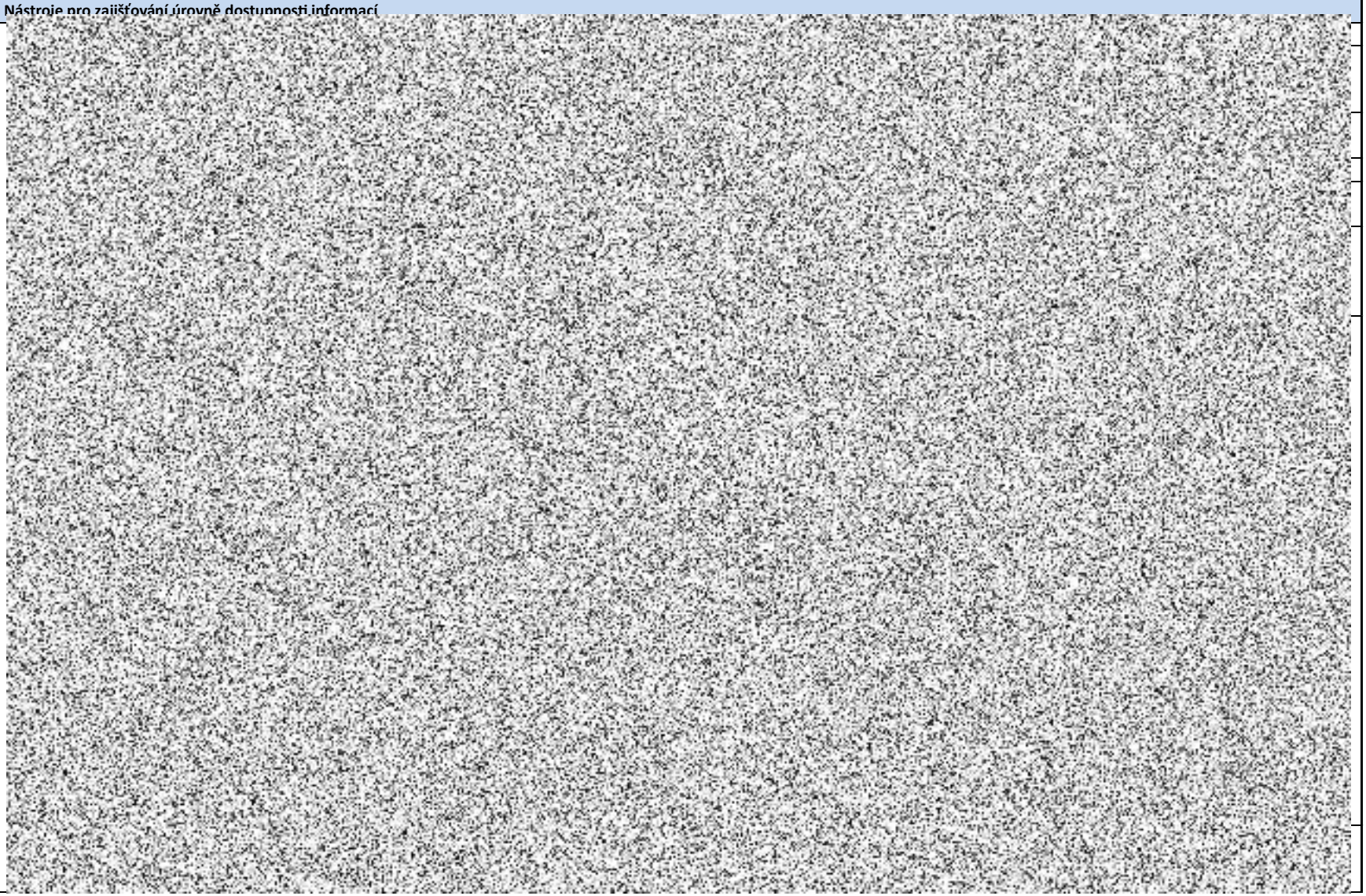
Komodita K.1 - Zvýšení zabezpečení komunikační sítě.	
	
Přístupový přepínač typ F 18x	

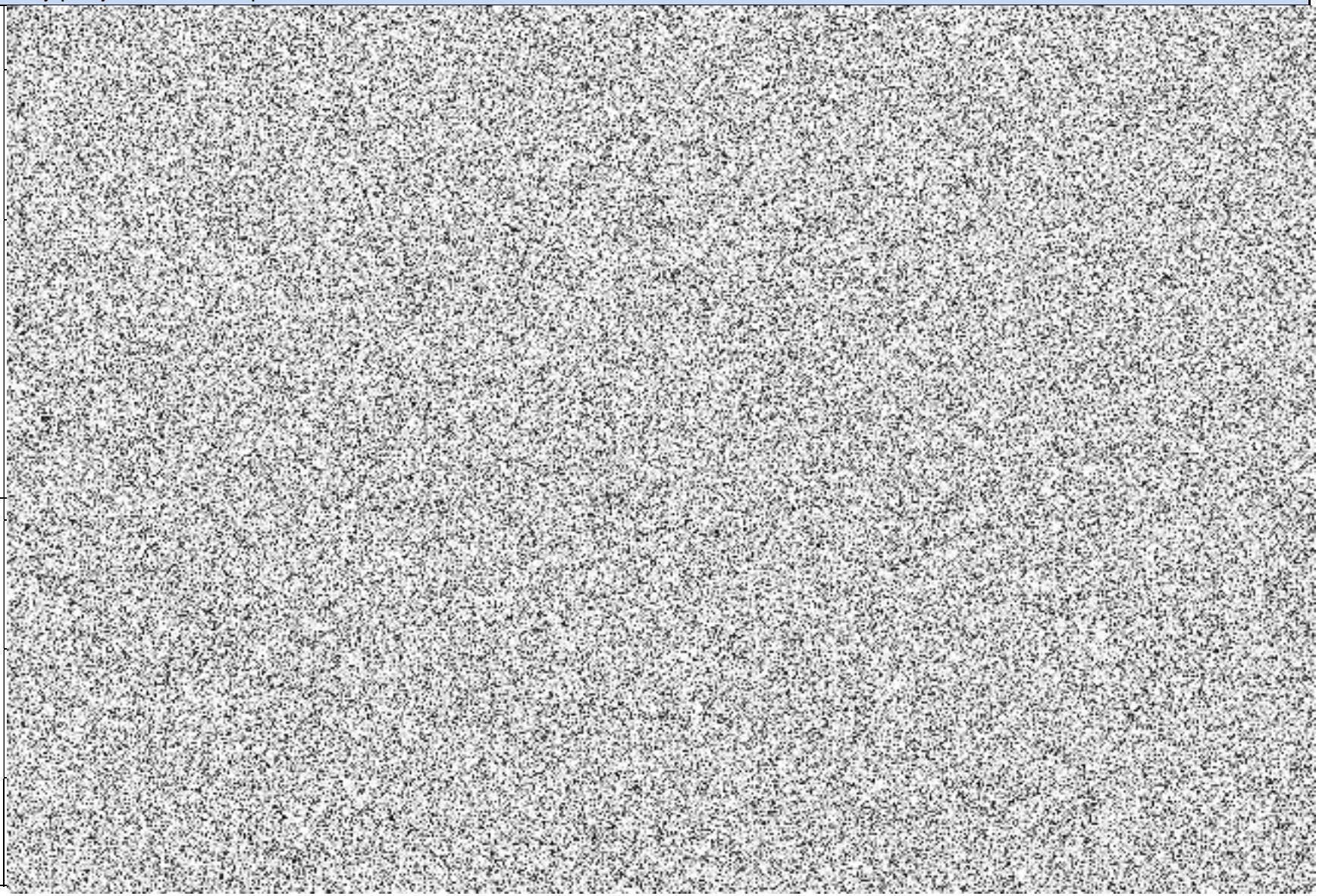
Komodita K.1 - Zvýšení zabezpečení komunikační sítě.	
	

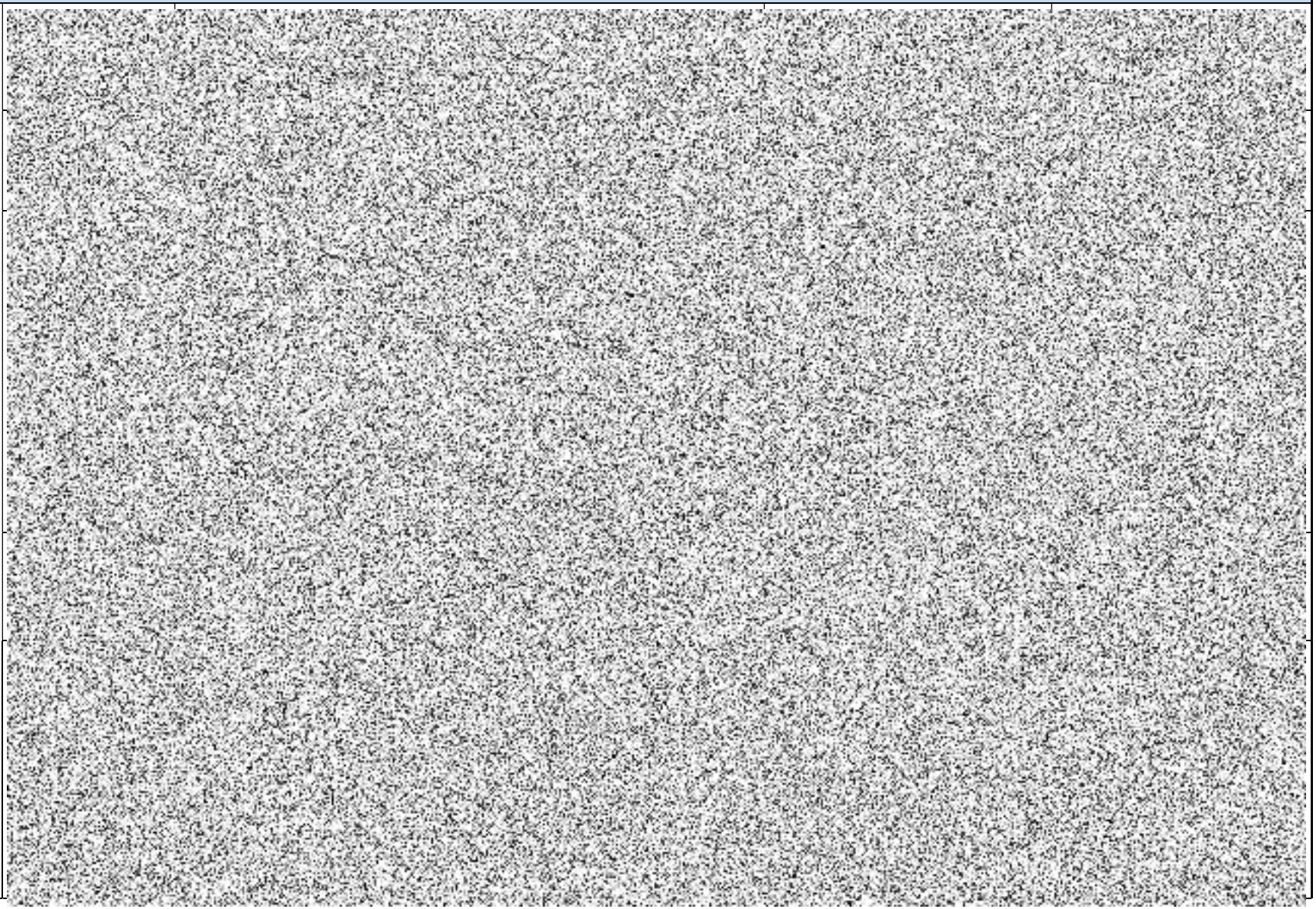
Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Bezpečné úložiště				

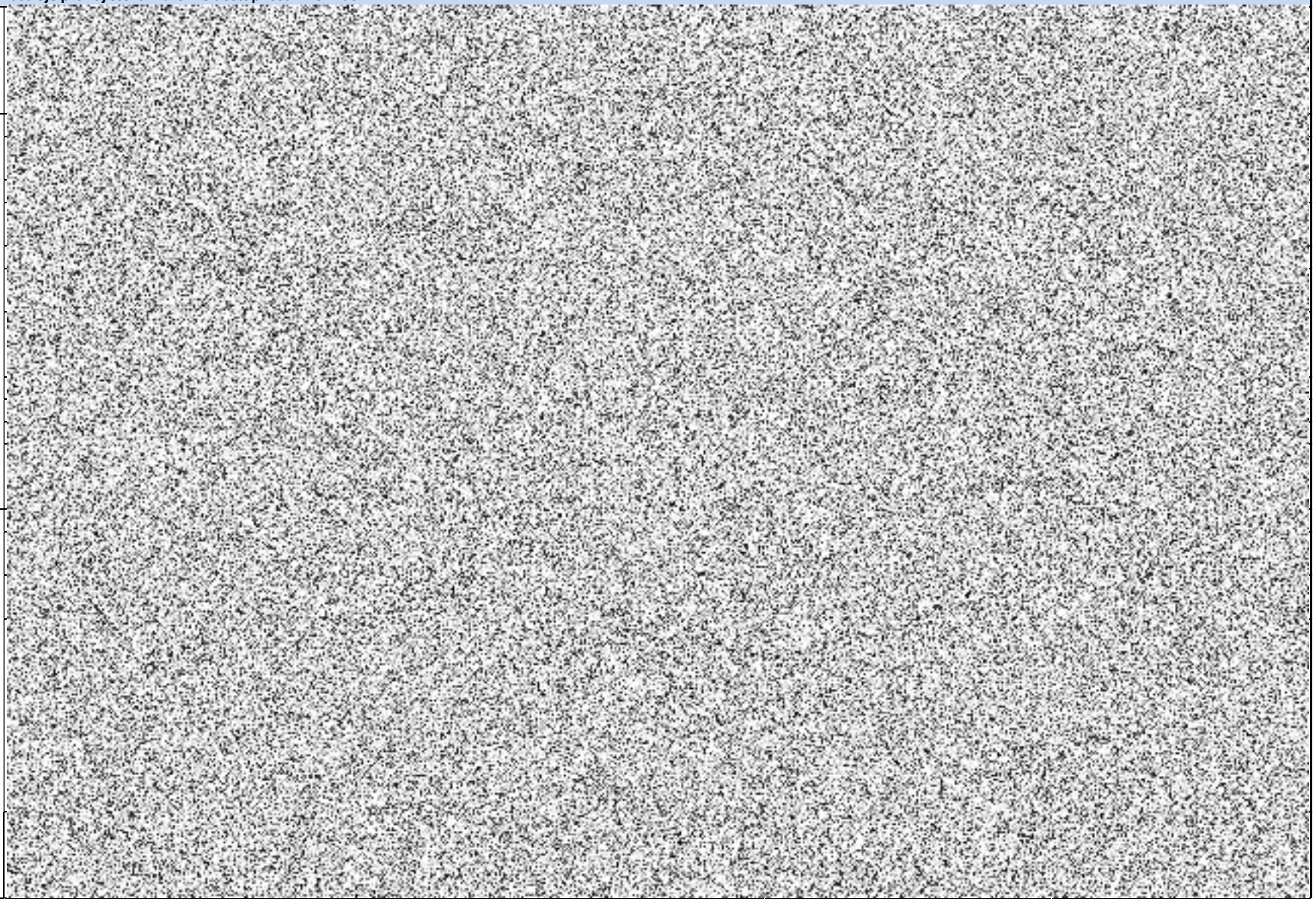
Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací	
	
Zálohovací server	

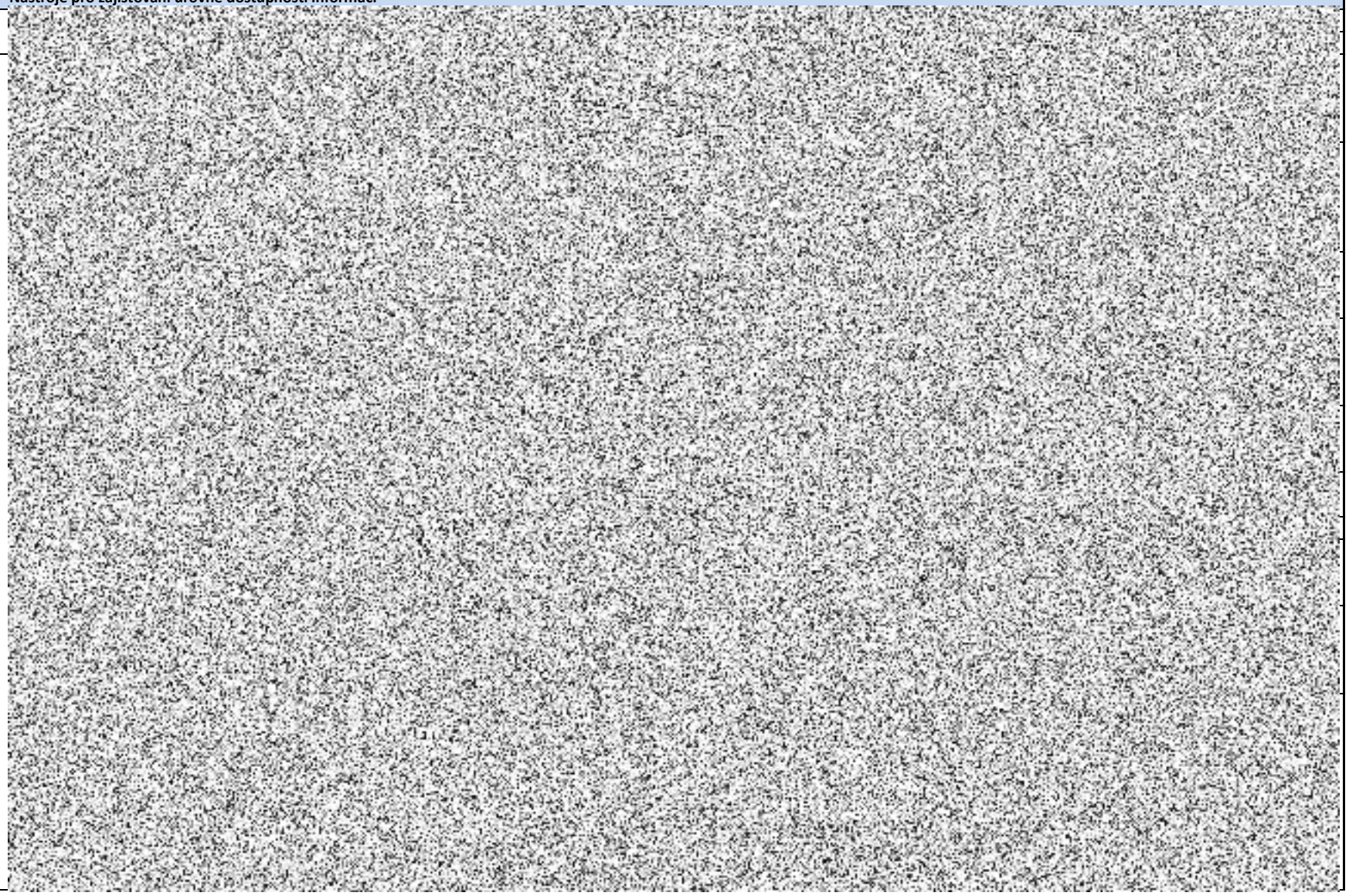
Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací

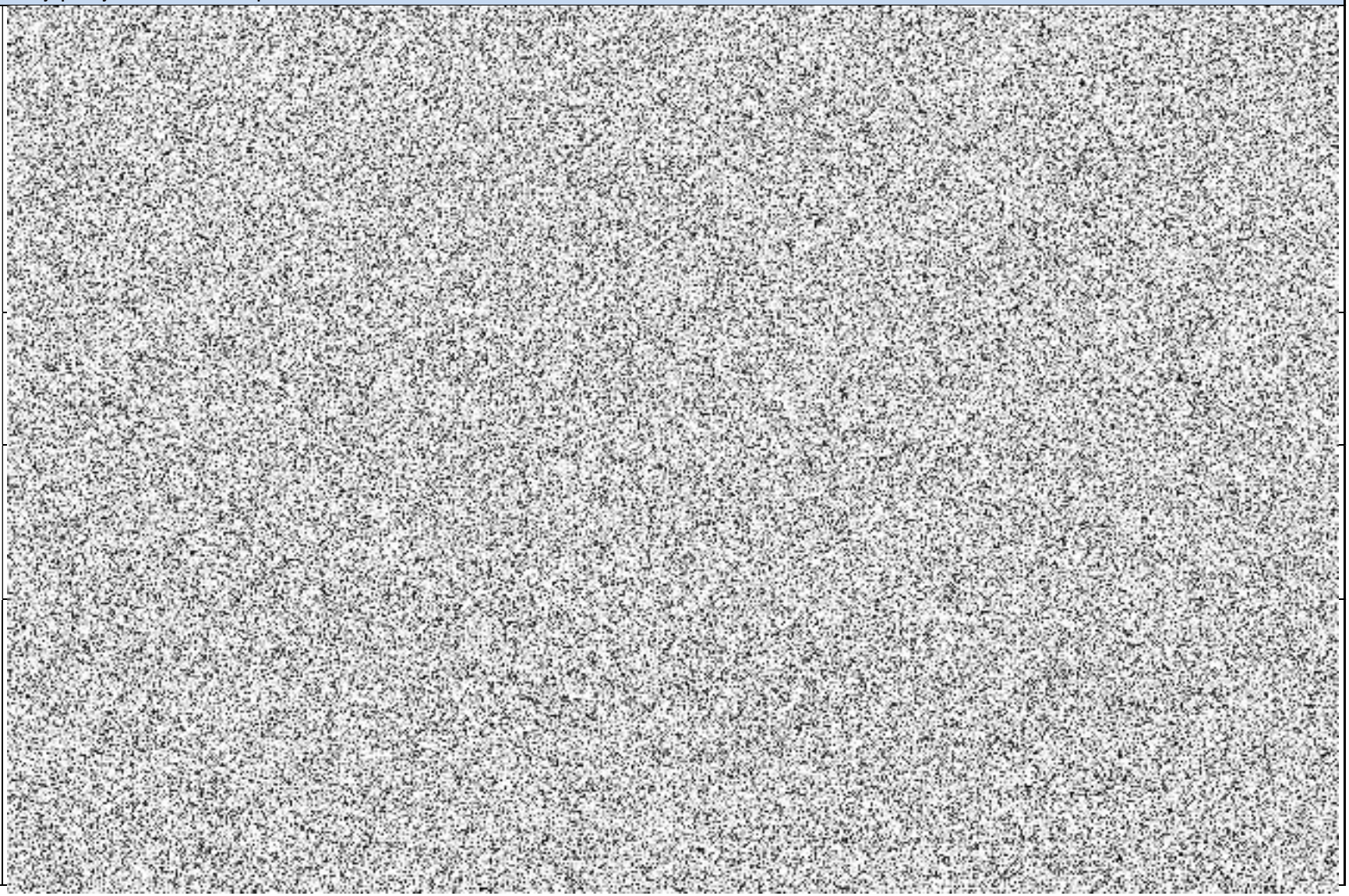


Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací	
	
Diskové úložiště	

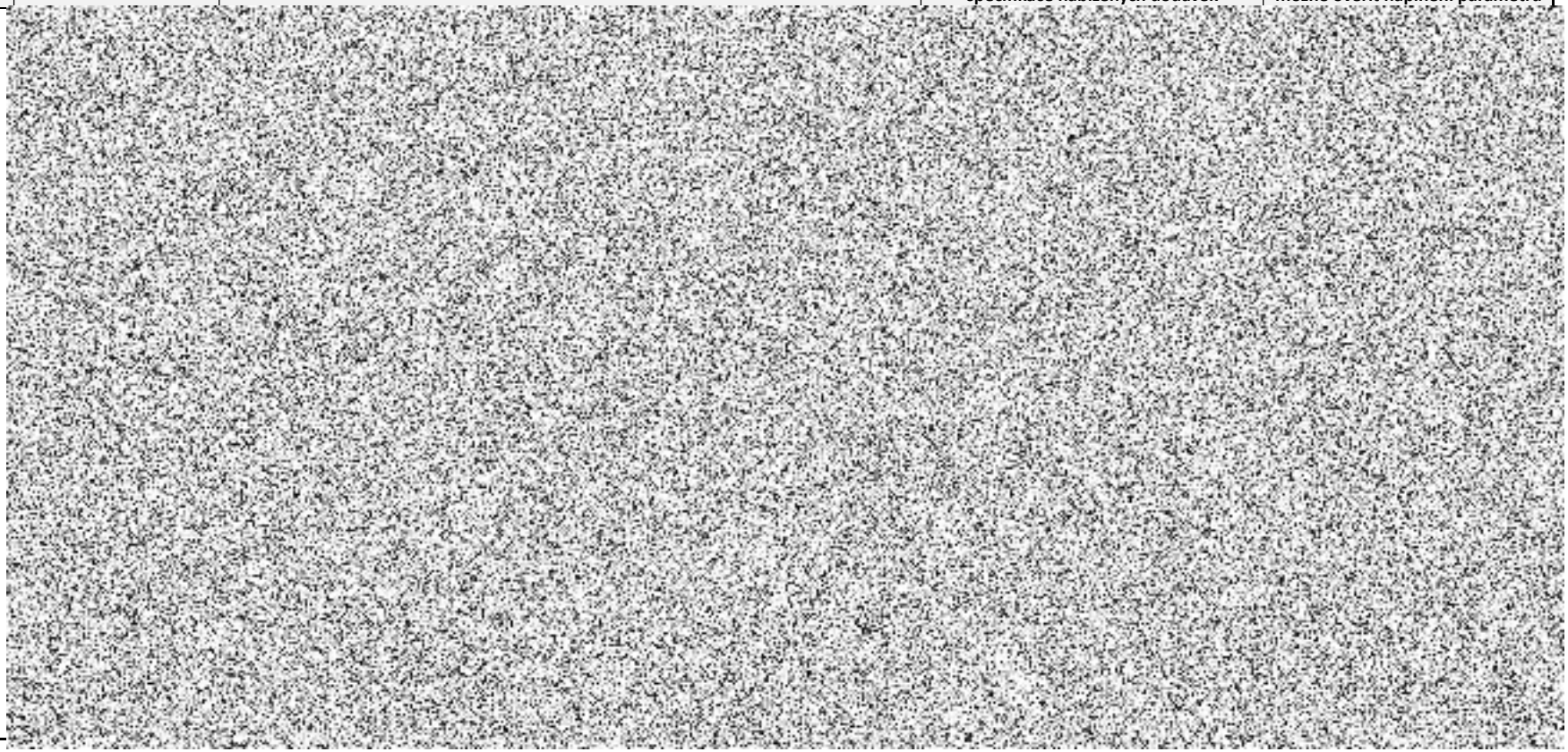
Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací	
	

Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací	
	
UPS	
PDU 2ks	

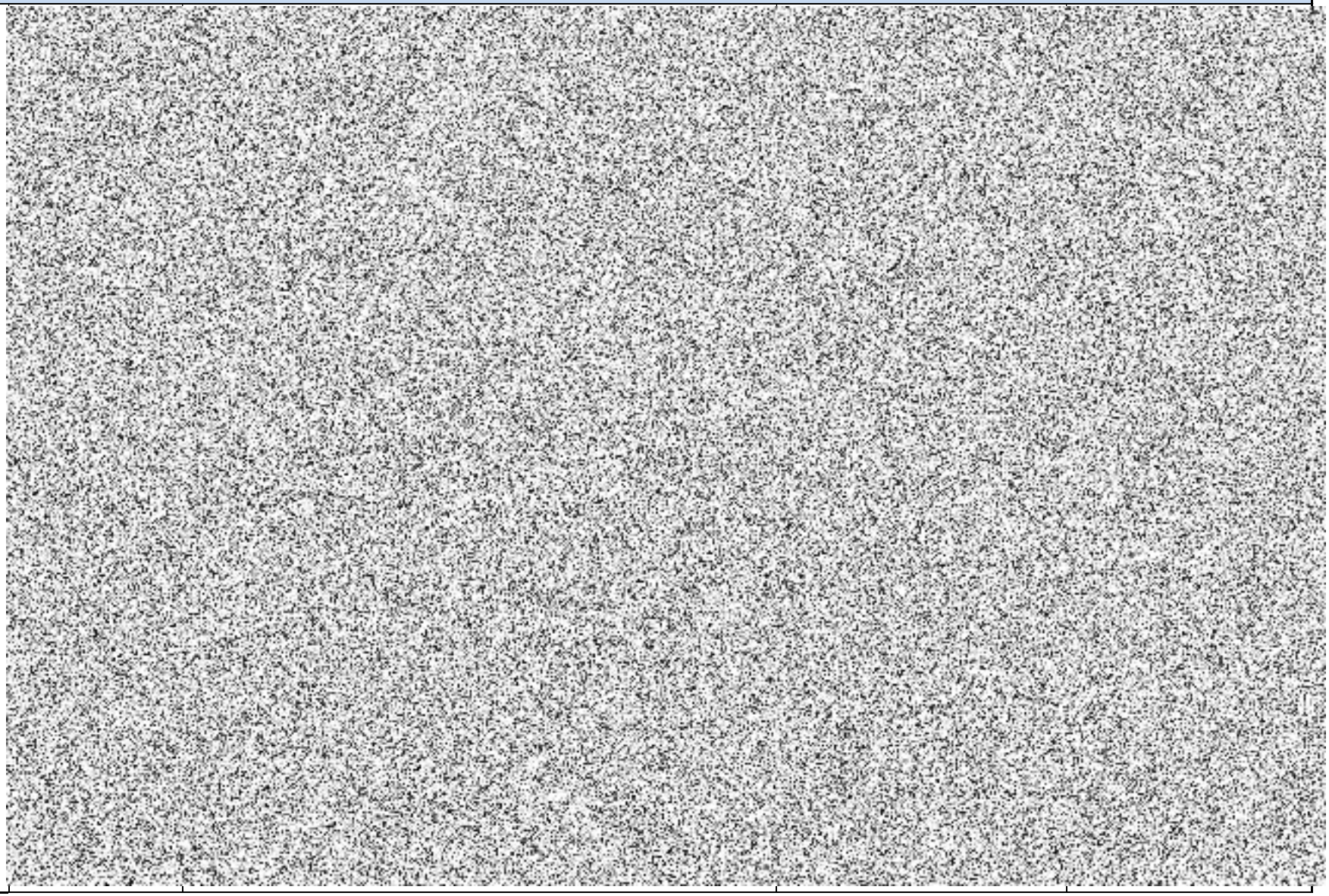
Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací	
	
Hypervisory 2ks	

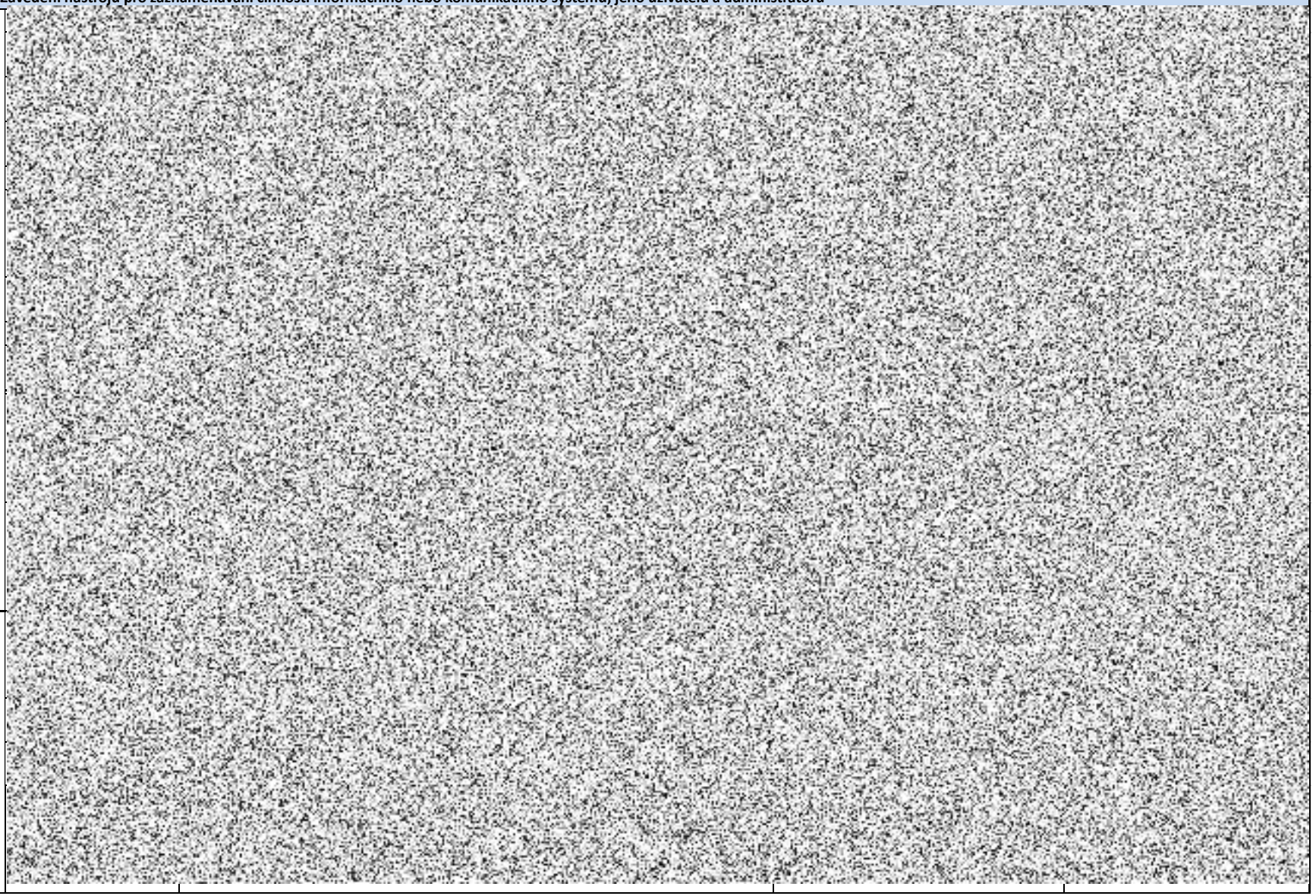
Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací	
	

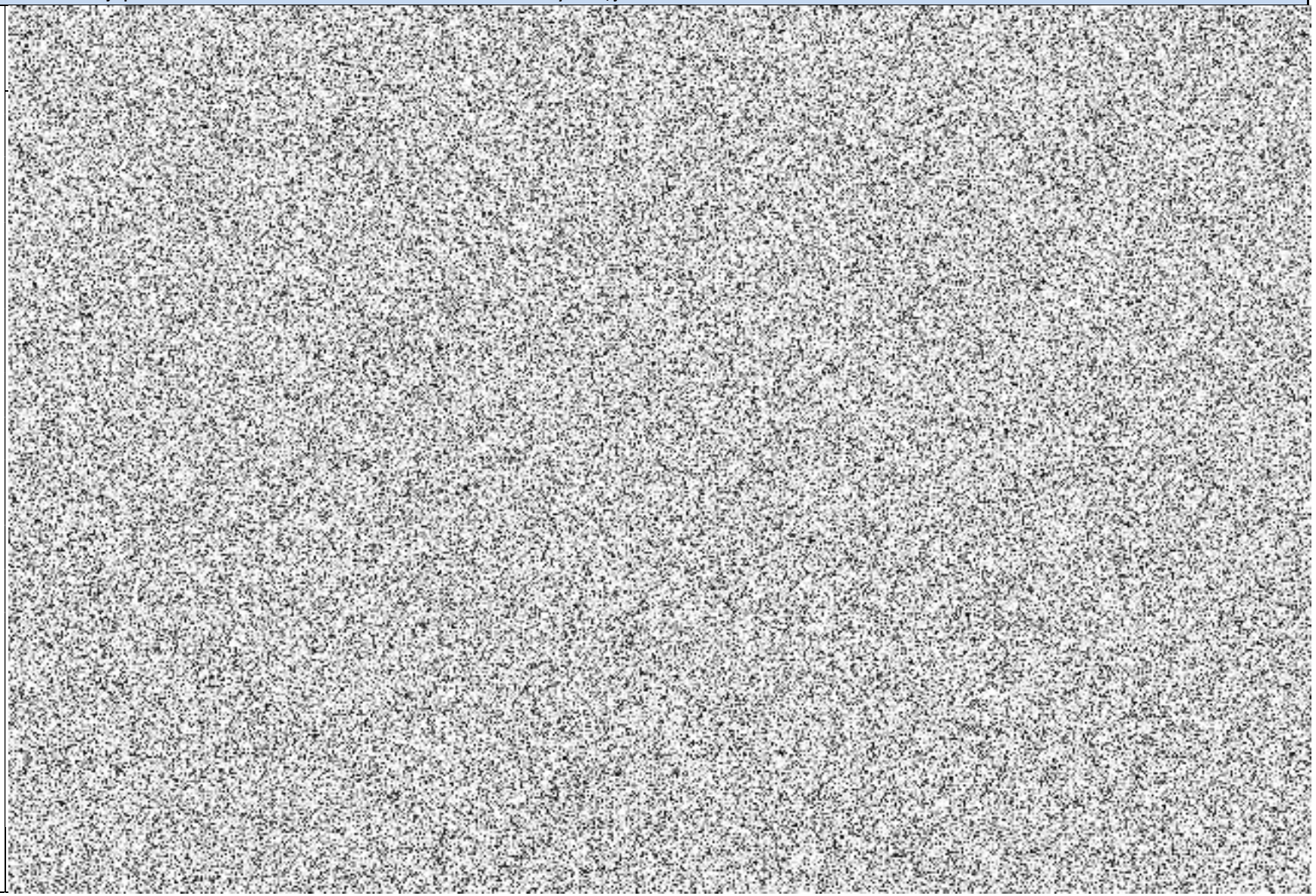
Komodita K.2 - Nástroje pro zajišťování úrovně dostupnosti informací	
Licence	

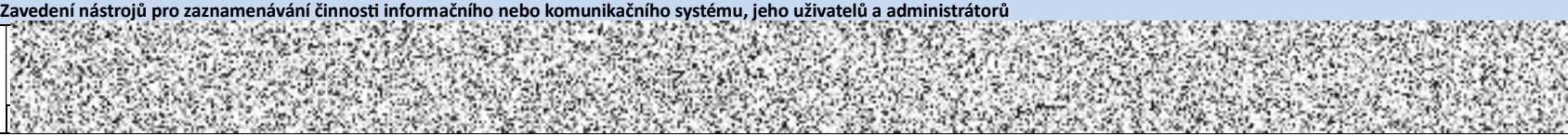
Komodita K.3 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů				
Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Systém pro správu logů				

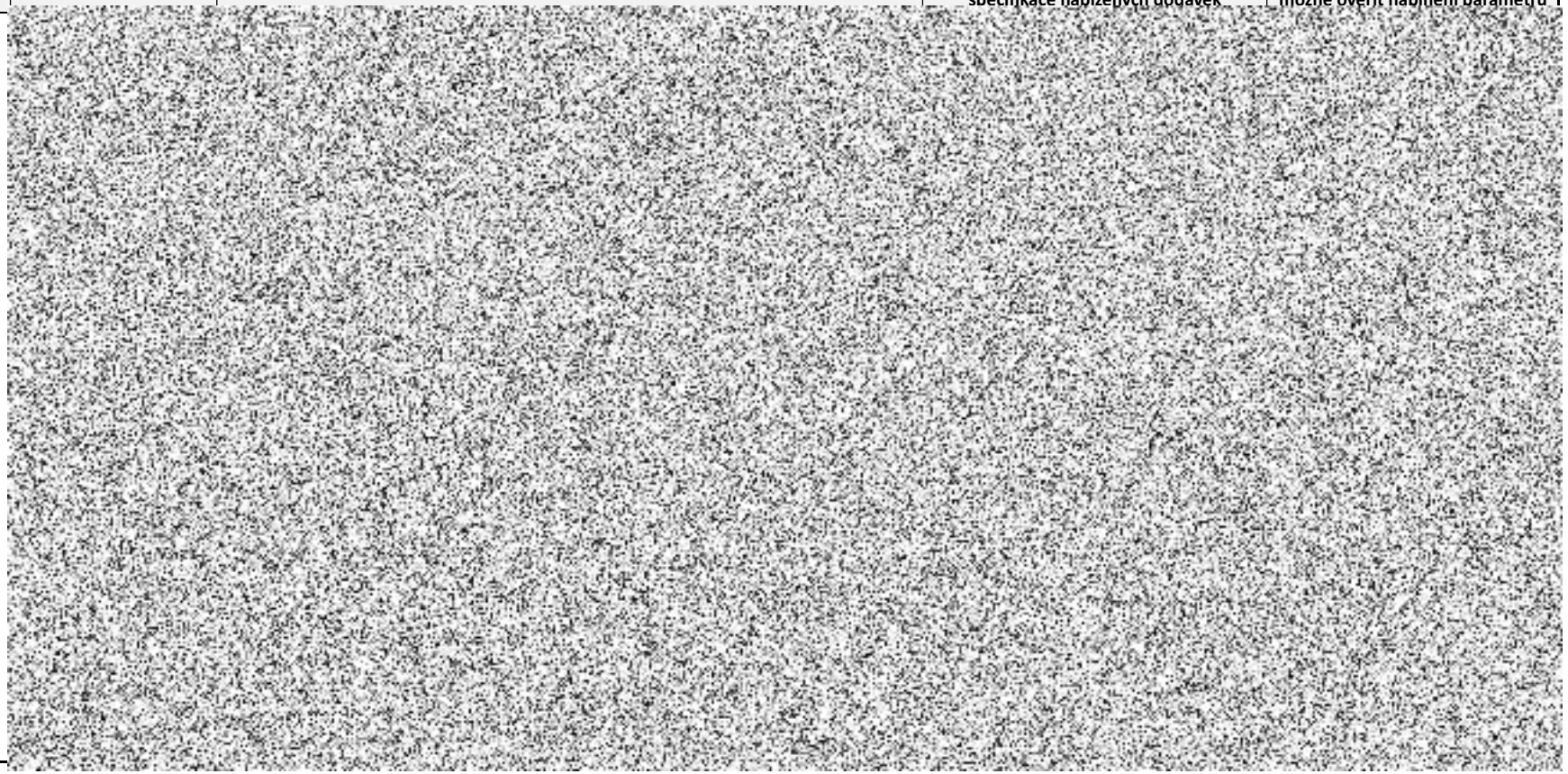
Komodita K.3 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

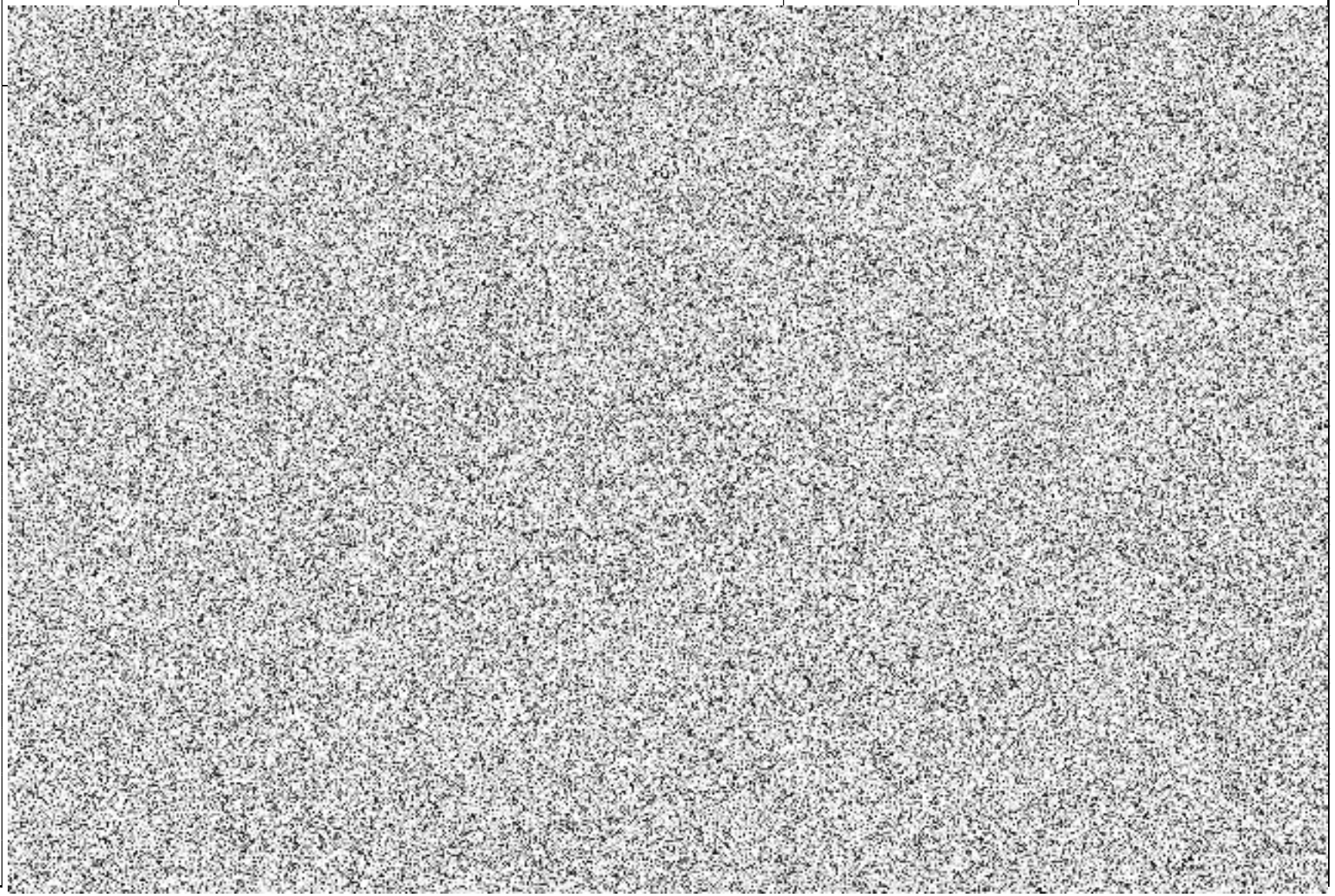


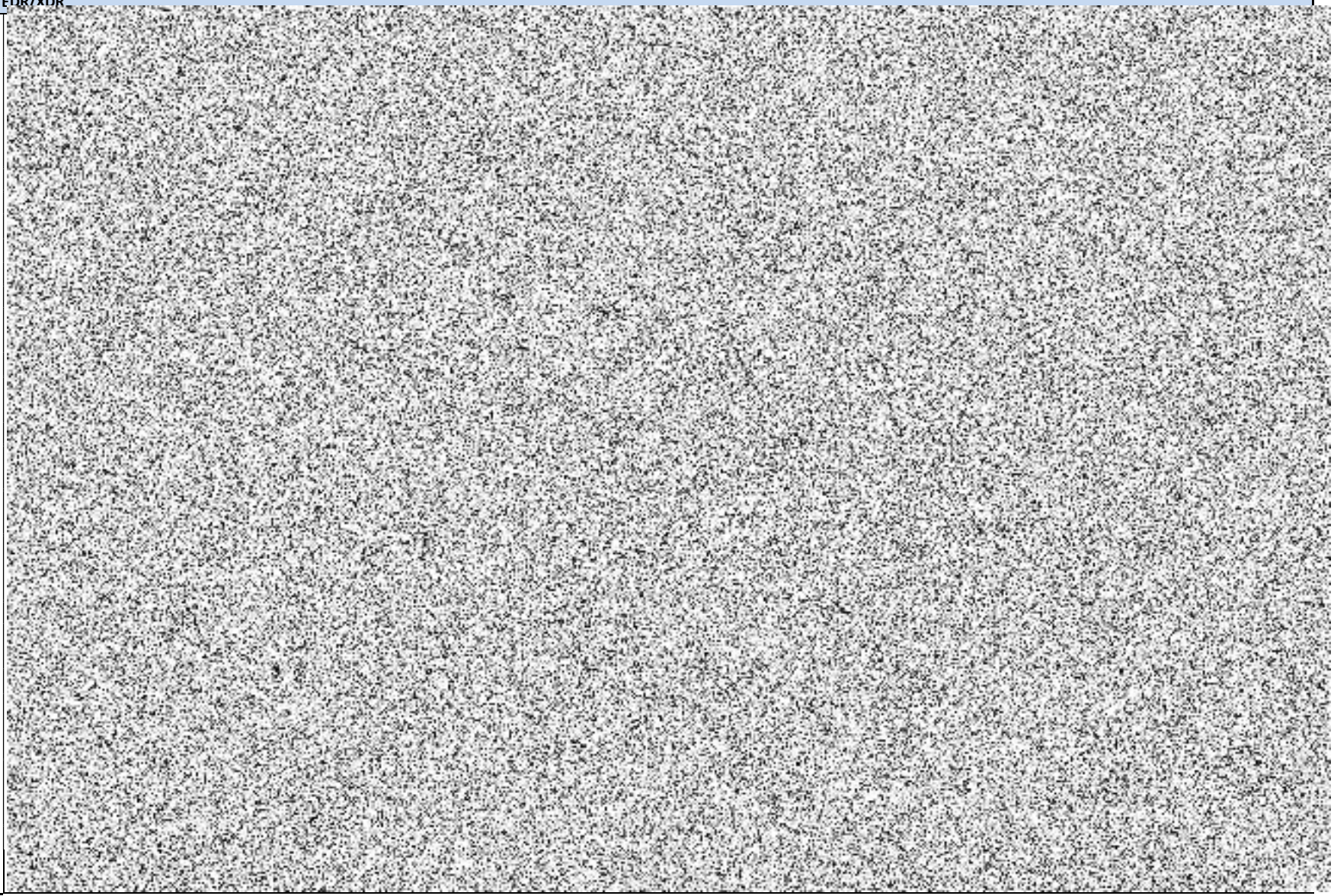
Komodita K.3 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů	
	
Audit AD	

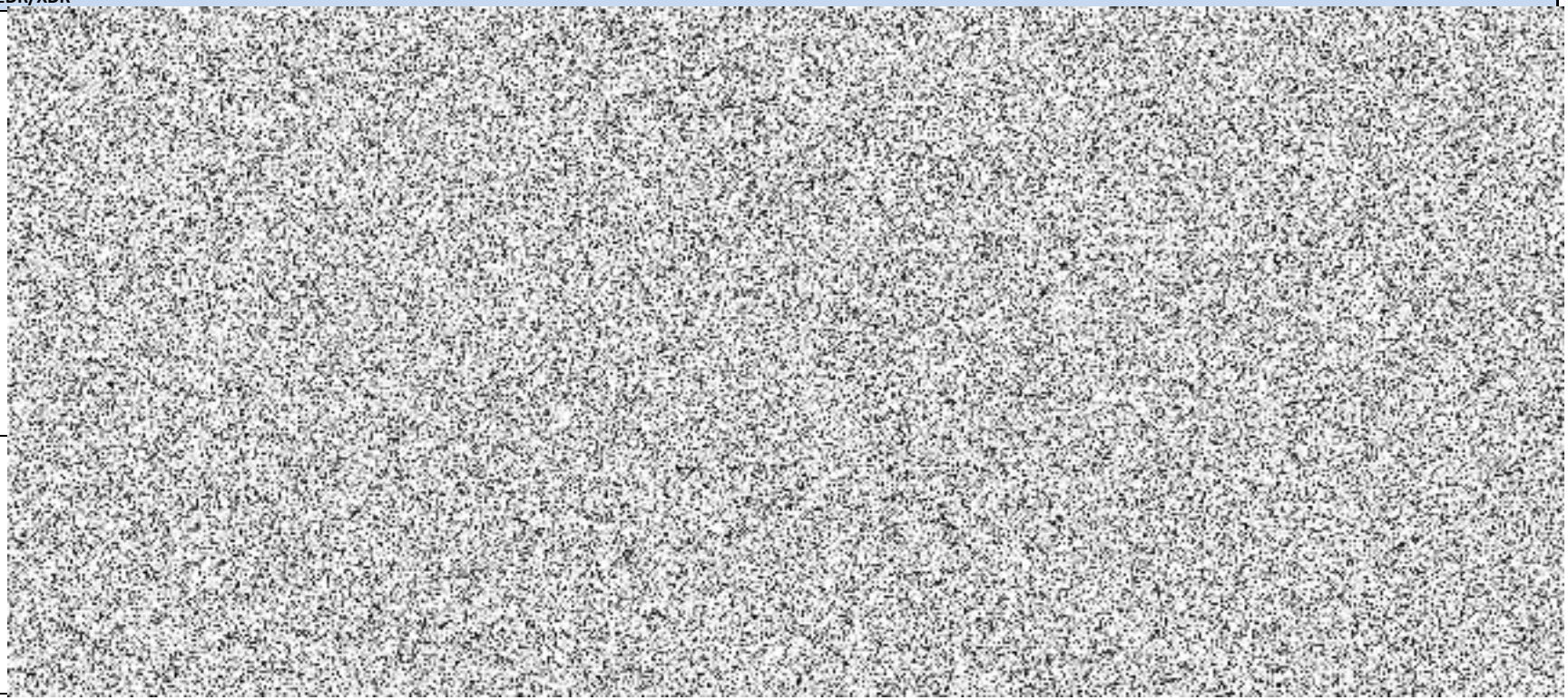
Komodita K.3 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů	
	

Komodita K.3 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů	
	

Komodita K.4 – EDR/XDR				
Část	**Parametr**	**Popis povinného parametru**	**Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
EDR/XDR				

Komodita K.4 – EDR/XDR	
	

Komodita K.4 – EDR/XDR	
	

Komodita K.4 – EDR/XDR	
	

2.7. Požadavky na architekturu technického řešení

(1) Architektura komodit musí být navržena tak, aby vhodně využívala a doplňovala stávající systémy ZUUL.

2.8. Požadavky na rozhraní

(1) Veškeré nabízené aktivní síťové prvky musí disponovat rozhraním SNMP min v2 pro management a vzdálenou správu.

2.9. Požadavky na kompatibilitu s ostatními systémy

(1) Veškeré softwarové komponenty nabízeného řešení budou provozovány ve virtuálním prostředí Microsoft Hyper-V a musí být pro běh v tomto prostředí výrobcem podporovány.

(2) Dodávaný zálohovací server, bezpečné datové úložiště, diskové úložiště a HW využívající Log/Event Management budou napojena do systému pro správu HW komponent Dell OpenManage, který zadavatel využívá. Napojení do řešení provede dodavatel. Dodavatel může nahradit stávající řešení Dell OpenManage za jiné, pokud bude zachována veškerá funkcionalita řešení Dell OpenManage.

(3) Veškeré dodávané technologie budou napojeny do monitorovacího systému Zabbix, který Zadavatel využívá. Napojení provede Dodavatel.

2.10. Požadavky na typy klientů

(1) Webová rozhraní nabízených systémů a zařízení být funkční v obvyklých internetových prohlížečích – min. Edge, Chrome, Safari v aktuálních verzích bez potřeby instalace speciálních doplňků či plug-in modulů.

2.11. Požadavky na bezpečnost informací

(1) Veškeré nástroje pro správu musí umožňovat správu interních účtů (min. jméno a heslo) a/nebo napojení na LDAP/Active Directory.

(2) Veškeré nástroje pro správu musí umožňovat definici s minimálně 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa)

(3) Veškeré nástroje pro správu musí komunikovat se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní hardware) musí být použita šifrovaná komunikace (např. HTTPS).

(4) Všechny software nástroje pro správu musí být schopné nasazení více faktorové autentizace pro přihlášení.

(5) Bezpečnost vnější komunikace publikovaných webových rozhraní aplikací a systémů bude v případě potřeby zajištěna použitím tzv. „hvězdičkového“ (wildcard) certifikátu veřejné certifikační autority, tj. takové autority, jejíž kořenový certifikát je součástí běžných operačních systémů a je automaticky obnovován v rámci běžných updatů operačních systémů. Účastník může využít stávající certifikát ZUUL nebo dodat jím preferovaný jako součást nabízeného řešení.

3. Implementační služby

3.1. Obecné požadavky

(1) Zadavatel požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Uchazeč je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné. Implementační služby budou minimálně v následujícím rozsahu:

(a) Zajištění projektového vedení realizace předmětu plnění dle standardu Prince 2 pro implementaci K1, K2 a K3.

(b) Zpracování prováděcí dokumentace, která představuje projektovou dokumentaci, podle které se projekt bude realizovat. Součástí zpracování prováděcí dokumentace je mj. provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.

(c) Dodávku nabízených prvků a kompletní implementaci řešení provedenou podle prováděcí dokumentace a splňující povinné parametry technického řešení,

(d) Provedení školení,

(e) Zajištění zkušebního provozu,

(f) Provedení akceptačních testů,

(g) Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby, administrace systémů a činností pro spolehlivé zajištění provozu a obnovu systémů K1, K2, K3, K4.

(h) Předání do ostrého provozu,

(2) Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

(3) Uchazeč je dále povinen zahrnout do nabídky i další související služby minimálně v dále uvedeném rozsahu. Pro každou uvedenou službu uvede uchazeč podrobný popis způsobu provedení služby při realizaci předmětu plnění zohledňující požadavky zadavatele na technické řešení.

K.1 - Zvýšení zabezpečení komunikační sítě
a) Analýza stávajícího síťového prostředí a návrh nové architektury LAN, WiFi, VPN b) Zavedení segmentace a IEE802.1X c) Výměna aktivních prvků d) Návrh a provedení akceptačních testů
K.2 - Nástroje pro zajišťování úrovně dostupnosti informací
a) Analýza současného způsobu ukládání a zálohování dat, návrh způsobu modernizace diskového úložiště a zálohování bez významného omezení provozu Zadavatele b) Provedení modernizace diskového úložiště v DC UnL, včetně upgrade hardware a firmware serverů a kompletní migrace dat c) Rekonstrukce zálohovacího systému se začleněním bezpečného úložiště d) Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a testy vysoké dostupnosti, dále obnovení min. 1 virtuálního serveru ze zálohy z každého úložiště záloh (tj. min 3 obnovy) e) Zapojení UPS a všech prvků v DC UnL, konfigurace virtualizační vrstvy, otestování výpadku el. energie.
K.3 - Zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů
a) Analýza a detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat, korelovat a analyzovat. Bude obsahovat i návrh způsobu zpracování získaných informací a vhodných proaktivních i reaktivních akcí b) Vybudování systému centrálního logování pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů

c) Návrh a provedení akceptačních testů, musí zahrnovat i testy archivace a obnovy logů a ověření detekce jejich neoprávněně modifikace. d) Nasazení auditování Active Directory se zaměřením na kontrolu privilegovaných účtů a kontrolu zranitelností AD. a) Nasazení více faktorové autentizace (MFA) pro přihlášení do obou systémů.
K.4 – EDR/XDR
b) Analýza současného stavu AV ochrany koncových zařízení c) Návrh na implementaci řešení EDR/XDR d) Návrh bezpečnostních doporučení nasazení EDR/XDR e) Instalace řešení, vytvoření vzorových politik f) Vzorová implementace na koncová zařízení g) Implementace na všechny zařízení h) Napojení na Log/Event Management (K.2) i) Nasazení více faktorové autentizace (MFA) pro přihlášení do centrální správy

(4) Uchazeč dle svého uvážení může doplnit v nabídce další služby, které jsou dle jeho názoru potřebné pro úspěšnou realizaci zakázky.

(5) Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (MS Office) používaných zadavatelem.

3.2. Požadavky na zpracování prováděcí dokumentace

(1) Uchazeč před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

(2) Jako podklad pro zpracování prováděcí dokumentace tedy uchazeč provede předimplementační analýzu, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění uchazeče, zejména pak s ohledem na uchazečem použité technické řešení, minimálně pro následující oblasti:

(a) Analýza a vyhodnocení stávajícího stavu, identifikace slabých míst a bezpečnostních rizik, včetně vazeb na HW a SW systémy.

(b) Způsob začlenění nabízených komodit do prostředí zadavatele.

(c) Síťová infrastruktura ve vztahu k plánovanému využití.

(d) Virtualizační infrastruktura (serverová, disková) ve vztahu k plánovanému využití.

(e) Analýza možností napojení zdrojových aplikačních systémů, resp. možností získávání jejich dat.

(f) Integrace nabízených softwarových systémů.

(g) Požadavky na rekonfiguraci stávajících systémů ve vztahu k plánovanému využití jejich dat.

(h) Dopady implementace na dostupnost a funkčnost stávajících služeb.

(i) Posouzení dopadů na non-IT technologie (spotřeba energií, tepelný výkon).

(j) Integrace s virtualizační platformou Hyper-V ve vysoce dostupném režimu a integrace s dohledovým systémem Zadavatele

(k) Požadované součinnosti Zadavatele.

(l) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

(3) Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného uchazečem a musí obsahovat minimálně tyto části:

(a) Detailní popis cílového stavu včetně funkcionalit jednotlivých částí systému,

(b) Nutné a doporučené optimalizační a konfigurační změny dodávaných systému i všech navázaných systémů (Hyper-V, LAN, VPN atd.),

(c) Způsob zajištění dodávek a služeb, včetně harmonogramu zajištění HW dodávek

(d) Způsob zajištění koordinace realizace předmětu plnění s běžným provozem,

(e) Detailní návrh a popis postupu implementace předmětu plnění,

(f) Detailní popis zajištění bezpečnosti informací,

(g) Detailní harmonogram projektu včetně uvedení kritických milníků,

(h) Vazby na stávající systémy a jejich konfigurace,

(i) Návrh akceptačních kritérií a akceptačních testů,

(j) Detailní popis navrhovaných školení,

(k) Komunikační schéma,

(l) Obsah a rozsah provozní dokumentace.

(4) Prováděcí dokumentace bude ve lhůtě do 10 pracovních dní od předání zhotovitelem připomínkována objednatelem a připomínky budou ze strany zhotovitele vypořádány v co nejkratší době s nástupem vypořádání do 2 pracovních dní (tj. zapracovány, případně s jasným a konkrétním písemným zdůvodněním odmítnuty jako nevalidní). Ze strany objednatele nebude v rámci připomínkování v případě nepravdivých, nepřesných nebo věcně nejasných informací v této dokumentaci požadováno její opravování na správné znění, bude se pouze jednat o vyznačení výše uvedených nedokonalostí a bude na zhotoviteli jejich řádné zpracování.

(5) **Prováděcí dokumentace musí být před zahájením realizace dalších etap plnění výslovně schválena zadavatelem**.

(6) Na základě provedené implementace bude prováděcí dokumentace aktualizována na skutečně provedenou včetně detailní konfigurace, a to jak funkční, tak provedené nastavení včetně podložení provedenými analytickými podklady a dokumenty. Aktualizovaná prováděcí dokumentace bude součástí dokumentace předávané v rámci předávacího protokolu.

3.3. Harmonogram realizace

(1) Uchazeč zajistí projektové vedení po celou dobu realizace zakázky osobou odpovědnou za realizaci předmětu plnění, která bude hlavní kontaktní osobou a která bude přítomna při všech jednáních týkajících se projektu.

(2) Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o dílo, čísla značí počet kalendářních dnů.

Poř. č.	Aktivita projektu	Nejpozdější termín pro dokončení aktivity
Etapa 1 - dodávky a implementace K.1-K.3		
E1.1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D+60
E1.2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+60
E1.3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+65
E1.4	Dodávky a implementace	D+200
E1.5	Školení uživatelů a administrátorů	D+200
E1.6	Zkušební provoz	D+200
E1.7	Akceptační testy	D+200

Poř. č.	Aktivita projektu	Nejpozdější termín pro dokončení aktivity
Etapa 1 - dodávky a implementace K.4		
E1.1	Předimplementační analýza a zhotovení Prováděcí dokumentace	D+60
E1.2	Předání Prováděcí dokumentace Zadavateli, připomínkové řízení	D+60
E1.3	Zapracování připomínek a předání finální verze Prováděcí dokumentace – akceptace Zadavatelem	D+65
E1.4	Dodávky a implementace	D+200
E1.5	Školení uživatelů a administrátorů	D+200
E1.6	Zkušební provoz	D+200
E1.7	Akceptační testy	D+200

(3) Uchazeč může dle svého uvážení výše uvedené maximální lhůty trvání v rámci Etapy 1 zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

(4) Maximální lhůty trvání nesmí uchazeč při tvorbě detailního harmonogramu prodloužit.

(5) Uchazeč uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy o dílo.

(6) Uchazeč uvede potřebnou součinnost zadavatele pro splnění harmonogramu plnění ve své nabídce.

3.4. Požadavky na školení

(1) Uchazeč zajistí školení pracovníků Zadavatele – administrátorů a uživatelů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

(2) Školení zajistí seznámení pracovníků Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin a pracovníkům bude vystaveno osvědčení o školení s uvedením rozsahu školení. Budou provedena tato školení:

(a) Školení administrátorů – minimální rozsah školení je 24 hodin, předpokládá se účast max. 4 účastníků, školení bude probíhat v sídle Zadavatele. Zadavatel může změnit místo školení dle potřeby.

(3) Náklady na školení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

(4) S ohledem na pandemii COVID-19 musí být formát školení připraven jak pro prezenční výuku, tak pro možnost provedení školení elektronicky (vzdálenou formou) např. pomocí MS Teams nebo jiných elektronických prostředí pro výuku. Formát školení bude zvolen zadavatelem nejpozději týden před realizací školení, a to podle aktuálního stavu pandemie a dle doporučení relevantních orgánů (Ministerstvo zdravotnictví ČR, Hygienická stanice atp.).

3.5. Výkonnostní testy diskového pole

Zadavatel požaduje provedení min. těchto výkonnostních testů diskového úložiště SSD:

Test	Požadavek min.
Test výkonosti kombinovaných IO operací	20 000 IO/s
Test propustnosti při sekvenčním čtení	900 MB/s
Test propustnosti při sekvenčním zápisu	550 MB/s

1. Test výkonosti kombinovaných IO operací
   Bude připraven testovací profil, který se bude skládat z mixu náhodných čtecích a zápisových operací (poměr čtení/zápis 66%/34%) o velikosti bloku 8 kB. Zátěž bude postupně navyšována (exponenciálně se zvyšující počet paralelních operací) do doby, než průměrná doba odezvy překročí hodnotu 20ms. Nejvyšší dosažená hodnota počtu IO operací bude brána jako výsledek.

2. Test propustnosti při sekvenčním čtení
   Bude připraven profil pro sekvenční čtení bloků o velikosti bloku 1 MB. Zátěž bude postupně navyšována (exponenciálně se zvyšující počet paralelních operací) do doby, než průměrná doba odezvy překročí hodnotu 20ms. Nejvyšší dosažená hodnota přenosové rychlosti [MB/s] bude brána jako výsledek.

3. Test propustnosti při sekvenčním zápisu
   Bude připraven profil pro sekvenční zápis bloků o velikosti bloku 1 MB. Zátěž bude postupně navyšována (exponenciálně se zvyšující počet paralelních operací) do doby, než průměrná doba odezvy překročí hodnotu 20ms. Nejvyšší dosažená hodnota přenosové rychlosti [MB/s] bude brána jako výsledek.

3.6. Požadavky na provedení akceptačních testů a přechod do zkušebního (testovacího) provozu

(1) Uchazeč navrhne způsob a provedení akceptačních testů. Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně:

(a) Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

(b) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

(c) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

(d) Prokázání registrace / aktivace podpory hardware a software výrobce, je-li podpora součástí dodávky a její aktivace potřebná

(e) Pro každou komoditu navrhne uchazeč vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a stabilita dodaného řešení.

(f) Výkonové testy prokazující shodu s požadovanými výkonnostními parametry a dále výrobcem deklarovanými či s ohledem na technologii objektivně očekávatelnými parametry, např. výkon u datových úložišť (IOPS, přenosová rychlost, latence)

(2) O provedení akceptace a jejím výsledku musí být vyhotoven písemný akceptační protokol. Šablony akceptačních protokolů budou předány zadavatelem při zahájení projektu, pro zapracování uchazečem do prováděcí dokumentace.

(3) Uchazeč zajistí pro každou komoditu zkušební (testovací) provoz v délce minimálně 30 dnů včetně technické podpory minimálně 1 specialisty na dodané řešení s dojezdem maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.

3.7. Požadavky na dokumentaci

(1) Uchazeč zpracuje provozní dokumentaci, která bude detailně popisovat konfiguraci zhotoveného díla a jeho vazby na stávající systémy.

(2) Provozní dokumentace bude vycházet z prováděcí dokumentace, která bude před předáním do provozu aktualizovaná dle skutečného stavu.

(3) Součástí provozní dokumentace bude popis úkonů doporučené údržby a specifikace intervalů jejích provádění a další dokumentaci v rozsahu stanoveném v prováděcí dokumentaci.

(4) Dokumentace bude dodána v elektronické podobě umožňující její zobrazení a čtení prostřednictvím běžných nástrojů typu kancelářského balíku nebo ve formátu PDF.

3.8. Technická kvalifikace

Zadavatel požaduje v souladu se zákonem o zadávání veřejných zakázek číslo 134/2016 Sb. ve znění pozdějších předpisů (dále též zákona) prokázání splnění technické kvalifikace dodavatele pro:

a) Komoditu K.1

§ 79 odst. 2 písm. b) zákona předložením

seznamu významných dodávek (vzor příloha 3 ZD) poskytnutých za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny, doby jejich poskytnutí a identifikace objednatele:

- Dodavatel do seznamu uvede **minimálně 2 (dvou) významných dodávek** týkajících NAC (HW – zejm. networking) v hodnotě min. 2 000 000 Kč bez DPH za každou z nich;

§ 79 odst. 2 písm. d) zákona předložením

osvědčení o vzdělání a odborné kvalifikaci vztahující se k předmětu veřejné zakázky, a to jak ve vztahu k fyzickým osobám, které mohou předmět veřejné zakázky poskytovat, tak ve vztahu k jejich vedoucím pracovníkům:

- Technický specialista networkingu
    - na pozici jsou kladeny následující minimální požadavky:
    - 3 roky praxe v oboru informačních technologií,
    - 2 referenční projekty obdobného zaměření jako předmět veřejné zakázky, na kterých se podílel v obdobné pozici,
    - prokázání dosažení certifikace pro návrh a implementaci nabízeného řešení a switchů.

b) Komoditu K.2

§ 79 odst. 2 písm. b) zákona předložením

seznamu významných dodávek (vzor příloha 3 ZD) poskytnutých za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny, doby jejich poskytnutí a identifikace objednatele:

- Dodavatel do seznamu uvede **minimálně 2 (dvou) významných dodávek** týkajících se vybudování nebo rekonstrukce virtualizační vrstvy (HW – zejm. severy, storage, networking, zálohování) v hodnotě min. 3 000 000 Kč bez DPH za každou z nich;

§ 79 odst. 2 písm. d) zákona předložením

osvědčení o vzdělání a odborné kvalifikaci vztahující se k předmětu veřejné zakázky, a to jak ve vztahu k fyzickým osobám, které mohou předmět veřejné zakázky poskytovat, tak ve vztahu k jejich vedoucím pracovníkům:

- Technický specialista zálohování – na pozici jsou kladeny následující minimální požadavky:
    - 3 roky praxe v oboru informačních technologií,
    - 2 referenční projekty obdobného zaměření jako předmět veřejné zakázky, na kterých se podílel v obdobné pozici,
    - prokázání dosažení certifikace na správu zálohovacího systému Veeam Backup & Recovery;
- Technický specialista datových úložišť – na pozici jsou kladeny následující minimální požadavky:
    - 3 let praxe v oblasti diskových datových úložišť a SAN,
    - 2 referenční projekty obdobného zaměření jako předmět veřejné zakázky, na kterých se podílel v obdobné pozici,
- Technický specialista software Microsoft–na pozici jsou kladeny následující minimální požadavky:
    - 3 let praxe v oboru informačních technologií;
    - 2 referenční projekty obdobného zaměření jako předmět veřejné zakázky, na kterých se podílel v obdobné pozici;
    - prokázání dosažení technické certifikace na správu a návrh designu platformy Microsoft min. v úrovni MCSE (Microsoft Certified System Engineer nebo Microsoft Certified Solutions Expert).
- Technický specialista síťových technologií–na pozici jsou kladeny následující minimální požadavky:
    - 3 roky praxe v oblasti datových sítí a aktivních prvků;
    - 2 referenční projekty obdobného zaměření jako předmět veřejné zakázky, na kterých se podílel v obdobné pozici;
    - prokázání dosažení certifikace pro návrh a implementaci nabízených switchů.
- Technický specialista datových úložišť (zejména ve vztahu k nabízenému diskovému poli) – na pozici jsou kladeny následující minimální požadavky:
    - 3 roky praxe v oblasti datových sítí a aktivních prvků;
    - 2 referenční projekty obdobného zaměření jako předmět veřejné zakázky, na kterých se podílel v obdobné pozici;
    - prokázání dosažení certifikace pro návrh a implementaci nabízené storage.

c) Komoditu K.3

§ 79 odst. 2 písm. b) zákona předložením

seznamu významných dodávek (vzor příloha 3 ZD) poskytnutých za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny, doby jejich poskytnutí a identifikace objednatele:

- Dodavatel do seznamu uvede **minimálně 2 (dvou) významných dodávek** týkajících zavedení nástrojů pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů (Log/Event Management), Zavedení nástroje pro auditování Active Directory v hodnotě min. 1 000 000 Kč bez DPH za každou z nich;

§ 79 odst. 2 písm. d) zákona předložením

osvědčení o vzdělání a odborné kvalifikaci vztahující se k předmětu veřejné zakázky, a to jak ve vztahu k fyzickým osobám, které mohou předmět veřejné zakázky poskytovat, tak ve vztahu k jejich vedoucím pracovníkům:

- Technický specialista Log managementu, AD Audit–na pozici jsou kladeny následující minimální požadavky:
  - 3 roky praxe v oboru informačních technologií,
  - 2 referenční projekty obdobného zaměření jako předmět veřejné zakázky, na kterých se podílel v obdobné pozici.
  - prokázání dosažení certifikace pro návrh a implementaci nabízeného řešení.
- Projektový manažer
  - 3 roky praxe v oboru informačních technologií,
  - 2 referenční projekty v oblasti informačních technologií, na kterých se podílel v obdobné pozici, ve výši minimálně 2 mil. Kč bez DPH za každý jednotlivý projekt,
  - prokázání dosažení certifikace projektového manažera dle IPMA, PMI, PRINCE2 nebo jiné rovnocenné metodiky projektového řízení na úrovni komplexního řízení projektů.

d) Komoditu K.4

§ 79 odst. 2 písm. b) zákona předložením

seznamu významných dodávek (vzor příloha 3 ZD) poskytnutých za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny, doby jejich poskytnutí a identifikace objednatele:

- Dodavatel do seznamu uvede **minimálně 2 (dvou) významných dodávek** týkajících zavedení nástrojů EDR/XDR v hodnotě min. 500 000 Kč bez DPH za každou z nich;

§ 79 odst. 2 písm. d) zákona předložením

osvědčení o vzdělání a odborné kvalifikaci vztahující se k předmětu veřejné zakázky, a to jak ve vztahu k fyzickým osobám, které mohou předmět veřejné zakázky poskytovat, tak ve vztahu k jejich vedoucím pracovníkům:

- Technický specialista EDR/XDR–na pozici jsou kladeny následující minimální požadavky:
  - 3 roky praxe v oboru informačních technologií,
  - 2 referenční projekty obdobného zaměření jako předmět veřejné zakázky, na kterých se podílel v obdobné pozici,
  - prokázání dosažení certifikace pro návrh a implementaci nabízeného řešení.

Příloha č.3 ke smlouvě SD2400251

ČESTNÉ PROHLÁŠENÍ

o opatřeních ve vztahu k mezinárodním sankcím přijatým Evropskou unií v souvislosti s ruskou agresí na území Ukrajiny vůči Rusku a Bělorusku

Číslo a název projektu:

CZ.06.01.01/00/22_003/0000035 Zvýšení kybernetické bezpečnosti Zdravotního ústavu se sídlem v Ústí nad Labem

Název veřejné zakázky: **ZUUL – Zvýšení kybernetické bezpečnosti**
(dále jen „veřejná zakázka“)

DODAVATEL

Dodavatel (název, IČO) Mepatek s.r.o., 27268080

Zastoupen (jméno příjmení, funkce): Daniela Dohnalová, jednatelka společnosti
(dále jen „dodavatel“)

Prohlašuji, že jako dodavatel veřejné zakázky nejsem dodavatelem ve smyslu nařízení Rady EU č. 2022/576, tj. nejsem:

a) ruským státním příslušníkem, fyzickou či právnickou osobou, subjektem či orgánem se sídlem v Rusku,
b) právnickou osobou, subjektem nebo orgánem, který je z více než 50 % přímo či nepřímo vlastněný některým ze subjektů uvedených v písmeni a), nebo
c) fyzickou nebo právnickou osobou, subjektem nebo orgánem, který jedná jménem nebo na pokyn některého ze subjektů uvedených v písmeni a) nebo b).

Prohlašuji, že nevyužiji při plnění veřejné zakázky poddodavatele, který by naplnil výše uvedená písm. a) – c), pokud by plnil více než 10 % hodnoty zakázky.

Dále prohlašuji, že neobchoduji se sankcionovaným zbožím, které se nachází v Rusku nebo Bělorusku či z Ruska nebo Běloruska pochází a nenabízím takové zboží v rámci plnění veřejných zakázek.

Současně prohlašuji, že žádné finanční prostředky, které obdržím za plnění veřejné zakázky, přímo ani nepřímo nezpřístupním fyzickým nebo právnickým osobám, subjektům či orgánům s nimi spojeným uvedeným v sankčním seznamu v příloze nařízení Rady (EU) č. 269/2014 ve spojení s prováděcím nařízením Rady (EU) č. 2022/581, nařízení Rady (EU) č. 208/2014 a nařízení Rady (ES) č. 765/2006 nebo v jejich prospěch[1].

V případě změny výše uvedeného budu neprodleně zadavatele informovat.

V Bystřanech dne 20.5.2024

Daniela Dohnalová, jednatelka společnosti

[1] aktuální seznam sankcionovaných osob je uveden na https://www.sanctionsmap.eu/