**UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI**


# Smernica č. 1/2018
# Prevádzkový poriadok Metropolitnej siete Univerzity Mateja Bela v Banskej Bystrici

Gestor: doc. Ing. Marek Drímal, PhD.
prorektor pre rozvoj a informatizáciu UMB

Schválil: doc. Ing. Vladimír Hiadlovský, PhD.
rektor UMB

Číslo záznamu: 3429/2018
Číslo spisu: 398 – 2018 – R – SR

Banská Bystrica 23. 4. 2018

## PRVÁ ČASŤ
## ÚVODNÉ USTANOVENIA

### Článok 1
### Účel smernice

1.1. Smernica Prevádzkový poriadok Metropolitnej siete Univerzity Mateja Bela v Banskej Bystrici (ďalej len „MS UMB") vymedzuje základné práva a povinnosti pre používateľov a správcov MS UMB.

1.2. MS UMB je budovaná a prevádzkovaná na podporu aktivít vykonávaných na Univerzite Mateja Bela v Banskej Bystrici (ďalej len „UMB") v súlade s odborným zameraním a spoločenským poslaním UMB. Tieto činnosti zahŕňajú, ale nie sú obmedzené na aktivity v oblasti správy, výučby, vedy a výskumu. MS UMB môže byť používaná len pre tieto účely a nesmie byť používaná na účely, ktoré nesúvisia s vyššie uvedenými aktivitami UMB.

1.3. Pravidlá uvedené v tomto poriadku nemusia predstavovať všetky pravidlá vzťahujúce sa k využívaniu MS UMB (t.j. v konkrétnych prípadoch je možné tieto pravidlá doplniť).

### Článok 2
### Vymedzenie základných pojmov

2.1. **IT systém** - súbor technických a programových prostriedkov, záznamových médií, dát a personálu, ktoré sa používajú na spracovanie informácií v určitej oblasti pôsobenia.

2.2. **Centrálny IT systém** – IT systém, ktorý prenáša, archivuje a spracováva údaje pre potreby celej inštitúcie alebo jej súčastí.

2.3. **Správca IT systému** - osoba, ktorá má na starosti správu, prevádzku, údržbu IT systému.

2.4. **Informačné a komunikačné technológie (ďalej len „IKT")** – technológie umožňujúce uchovávanie, spracovávanie, šírenie a prezentáciu informácií v digitálnej alebo elektronickej forme.

2.5. **Správca IKT** – správca hardvéru a softvéru patriaceho organizačnej súčasti UMB, ktorý zároveň poskytuje podporu pri práci s IKT pre koncových používateľov (zamestnancov, doktorandov a študentov).

**2.6. IT bezpečnostný správca** – IT bezpečnostným správcom je riaditeľ UAKOM.

2.7. **Chránené údaje** – údaje, ktoré je nutné chrániť, aby k nim nemala prístup neoprávnená osoba. Príkladom chránených údajov sú prihlasovacie údaje používateľa MS alebo také údaje, ktoré majú dopad na práva a slobody dotknutých fyzických osôb alebo údaje, ktorých šírenie je UMB považované za nevhodné. Osobné údaje definované legislatívou SR a EÚ sú tiež považované za chránené údaje.

2.8. **Chránená pracovná stanica** – pracovná stanica, ktorá obsahuje chránené údaje.

2.9. **UMB Office 365** – Produkt Office 365 Education Plus od spoločnosti Microsoft na základe zmluvy Campus Agreement (alebo jej nástupníckymi zmluvami) uzatvorenou medzi spoločnosťou Microsoft a Ministerstvom školstva, vedy, výskumu a športu SR. Jedná sa o balík najmä cloudových služieb a nástrojov poskytovaný študentom a zamestnancom UMB.

2.10. **Virtuálna privátna sieť (ďalej len „VPN")** – je súčasť siete UMB, ktorá umožňuje zabezpečený prístup k serverom a pracovným staniciam z prostredia mimo UMB.

2.11. **Konto UMB** - slúži na prihlásenie do IT systémov UMB.

2.12. **Metropolitná sieť Univerzity Mateja Bela v Banskej Bystrici (ďalej len „MS UMB")** - je celouniverzitná počítačová sieť, ktorá je základom IT a komunikačného systému UMB. Správcom MS UMB je Ústav automatizácie a komunikácie UMB (ďalej len „UAKOM"). Pri nahlasovaní problémov súvisiacich s MS UMB sa postupuje v zmysle článku 16 tejto smernice.

2.13. **Správca siete** – správcom siete sa myslí správca MS UMB.

2.14. **Metropolitná optická sieť Univerzity Mateja Bela v Banskej Bystrici (ďalej len „MOS UMB-NET")** – metropolitná optická sieť Univerzity Mateja Bela v Banskej Bystrici.

2.15. **Prevádzkové údaje** - údaje vzťahujúce sa na používateľa a na konkrétny prenos informácií v sieti. Tieto údaje vznikajú v procese prenosu informácií a zaznamenávajú sa na účely prenosu správy v sieti (IP a MAC adresa pripájaného zariadenia, cieľová IP adresa, dátum, čas a trvanie komunikácie, v prípade sieťových služieb viazaných na overenie /autentifikáciu používateľa aj prihlasovacie meno).

2.16. **Šifrovanie dát** – šifrovanie je postup, ktorý zabezpečí aby dáta neboli čitateľné pre neautorizovanú osobu.

2.17. **Používateľ Metropolitnej siete Univerzity Mateja Bela v Banskej Bystrici (ďalej len „používateľ MS UMB" alebo „používateľ MS")** – zamestnanci, študenti, účastníci konferencií alebo akýkoľvek iný používatelia zariadení, ktoré sa pripájajú do MS.

2.18. **Lokalizačné údaje** - údaje zaznamenané v elektronickej komunikačnej sieti alebo prostredníctvom elektronickej komunikačnej služby, ktoré označujú geografickú polohu koncového zariadenia používateľa (pri pripojení do káblovej siete je to identifikácia sieťovej zásuvky, pri pripojení do bezdrôtovej siete je to identifikácia prístupového bodu).

## DRUHÁ ČASŤ
## METROPOLITNÁ SIEŤ UMB A PRÁCA V NEJ

### Článok 3
### Práva a povinnosti používateľov MS UMB

3.1. Používateľ MS UMB má právo na používanie MS UMB jedine na pracovné, študijné alebo výskumné účely. Používanie MS UMB na pracovné účely zahŕňa všetky aktivity, ktoré zamestnanci UMB realizujú prostredníctvom MS UMB pri plnení pracovných úloh v rozsahu definovanom pracovnou náplňou zamestnanca. Používanie MS UMB na študijné účely zahŕňa všetky aktivity, ktoré študenti a doktorandi UMB realizujú prostredníctvom MS UMB s cieľom splniť podmienky štúdia podľa študijného programu v zvolenom študijnom odbore, v zmysle zákona č. 131/2002 Z. z. o vysokých školách. Používanie MS UMB na výskumné účely zahŕňa všetky aktivity, ktoré zamestnanci, študenti a doktorandi UMB realizujú prostredníctvom MS UMB pri riešení úloh a projektov v oblasti vedy a výskumu.

3.2. Používateľ MS má právo na pridelenie prístupových práv k prvkom siete MS UMB podľa pravidiel, ktoré stanovuje táto smernica. Prístupové práva používateľa MS sú viazané na jeho používateľské konto a sú dané jeho individuálnou alebo skupinovou identifikáciou (napr. správa UMB, pedagóg, študent, výskum, iná kategória, atď.). Pravidlá pre vytváranie konta a jeho používanie sú uvedené v čl.5 tejto smernice.

3.3. Používateľ MS nesie plnú zodpovednosť za svoje aktivity v MS UMB a v počítačových sieťach, do ktorých má prístup cez MS UMB.

3.4. Používateľ MS je povinný pri komunikácii s inými sieťami prostredníctvom MS UMB dodržiavať pravidlá, ktoré platia v týchto sieťach.

3.5. Používateľ MS sa nesmie žiadnymi prostriedkami pokúšať o získanie prístupových práv alebo privilegovaných stavov, ktoré mu neboli pridelené správcom sieťového prvku alebo IT systému. Pokiaľ používateľ MS akýmkoľvek spôsobom (napr. v dôsledku chyby technických alebo programových prostriedkov) získa privilegovaný stav alebo prístupové práva ktoré mu neboli pridelené, nesmie túto skutočnosť zneužiť a je povinný to bezodkladne oznámiť príslušnému správcovi.

3.6. Používateľ MS sa nesmie pokúšať získať prístup k chráneným informáciám a dátam (resp. dátovej komunikácii) iných používateľov. Všetky dáta obsiahnuté v zariadeniach MS UMB treba považovať

za dôverné, pokiaľ nie je explicitne uvedené alebo z ich povahy zrejmé (napr. obsah verejných webových stránok fakulty), že sú určené pre všeobecnú a neobmedzenú distribúciu.

3.7. V záujme plnenia cieľov uvedených v tejto smernici môže v odôvodnených prípadoch správca dotknutého IT systému obísť nariadenie uvedené v bode 3.6. V takom prípade je povinný zaznamenať svoj postup, informovať o ňom svojich nadriadených.

3.8. Používateľ MS nesmie napomáhať iným osobám pri získavaní prístupových práv alebo privilegovaných stavov, ktoré im neboli pridelené správcom sieťového prvku, ani pri získavaní prístupu k chráneným informáciám a dátam iných používateľov MS.

3.9. Používateľ MS pri práci v sieti UMB nesmie aktívne utajovať svoju identitu. Je zakázané používať falošnú identitu (vydávať sa za iného používateľa MS).

3.10. Používateľ MS nikdy nesmie v sieti vykonávať takú činnosť, ktorá by ostatným používateľom MS bránila v riadnom používaní siete, napr. nadmerným zaťažovaním prvkov siete (k čomu môže dochádzať pri používaní peer-to-peer sietí ako BitTorrent).

3.11. Je zakázané vykonávať prenosy dát, ktoré sú v rozpore s autorskými právami alebo platnou legislatívou SR a EÚ (sťahovanie a šírenie nelegálnych kópií komerčného softvéru, audio a video záznamov atď.).

3.12. Používateľ MS nesmie prenášať, používať a šíriť programové vybavenie v rozpore s jeho licenčnými podmienkami. Používateľ MS nesmie kopírovať a distribuovať časti operačného systému a inštalovaných programov bez súhlasu príslušného správcu.

3.13. Používateľ MS nesmie používať MS UMB na politickú a náboženskú agitáciu. Je zakázané používať v rámci MS UMB vulgárne a znevažujúce výrazy v komunikácii, ktorá je určená pre väčší okruh ľudí (napr. webové stránky, elektronické konferencie, atď.) a prenášať, uskladňovať alebo vystavovať informácie, ktoré sú v rozpore s platnými právnymi predpismi a všeobecne akceptovanými spoločenskými normami (napr. nepovolená reklama, rasové útoky, obscénne materiály, psychický teror, nelegálne kópie zvukových alebo obrazových záznamov).

3.14. Používateľ MS nesmie svojvoľne meniť konfiguráciu sieťových prvkov, pracovných staníc a ďalších zariadení v MS UMB. Všetky zmeny konfigurácie môžu byť vykonávané len so súhlasom príslušného správcu IKT alebo IT systému a s ohľadom na prevádzku siete.

3.15. Akékoľvek svojvoľné pripájanie, odpájanie a premiestňovanie sieťových prvkov je prísne zakázané.

3.16. Pripojenie zariadenia, ktoré nie je vo vlastníctve UMB resp. fakúlt, (napr. vlastný prenosný počítač) do siete UMB je možné len so súhlasom príslušného správcu lokálnej siete, do ktorej sa zariadenie pripája. Správca je v takom prípade povinný overiť správnosť nastavenia (konfigurácie) zariadenia pre prácu v sieti. Táto možnosť sa vzťahuje na zamestnancov v pracovnom pomere s UMB v Banskej Bystrici alebo s jej fakultami a organizačnými zložkami. Študenti majú takúto možnosť len v tom prípade, ak vo vyhradených priestoroch (počítačové učebne pre študentov) sú k dispozícii prípojné zásuvky vyhradené na tento účel. Pripojené zariadenie nesmie nijakým spôsobom narušiť prevádzku siete a najmä jej bezpečnosť. Vlastník zariadenia nesie plnú zodpovednosť za problémy, ktoré zariadenie po pripojení do siete spôsobí. Správca IKT nie je povinný riešiť prípadné problémy vzniknuté na takomto zariadení po jeho pripojení do siete.

3.17. Akékoľvek overovanie a zavádzanie nových sieťových služieb a činností v MS UMB je možné len so súhlasom správcu MS UMB. Používatelia MS žiadajú o tento súhlas prostredníctvom správcov IKT.

3.18. Ak používateľ MS zistí nejakú poruchu na sieťovom prvku, je povinný to oznámiť ihneď príslušnému lokálnemu správcovi IKT alebo vedeniu UAKOM.

3.19. Je zakázané využívať MS UMB na súkromné aktivity.

3.20. V nepretržitej prevádzke resp. mimo bežnej pracovnej doby môžu bez dozoru pracovať len vyhradené počítače (servery) umiestnené vo vyhradených priestoroch (miestnosti serverov, správcov sietí, komunikačné uzly). V záujme zaistenia bezpečnosti prevádzky dátovej siete a tiež protipožiarnej bezpečnosti je zakázané nechávať zapnuté počítače v kanceláriách a učebniach mimo pracovnej doby bez dozoru. V odôvodnených prípadoch (napr. rozsiahle matematické, štatistické výpočty) je možné nechať počítač v prevádzke bez dozoru v mimopracovnej dobe, ale pri zachovaní potrebných zásad protipožiarnej bezpečnosti a tiež bezpečnosti prevádzky dátovej siete. O takomto používaní počítača je používateľ MS povinný vopred informovať správcu siete.

3.21. Používateľ MS môže v odôvodnených prípadoch (napr. služobná cesta v zahraničí) požiadať o prístup do MS UMB zo sieťových prvkov mimo MS UMB.

3.22. Používateľovi MS, ktorý tento Prevádzkový poriadok poruší, môže správca obmedziť dočasne alebo trvalo jeho prístup k sieti UMB. Stupne obmedzenia prístupu sú nasledovné:

a) podmienečné zablokovanie prístupu;
b) dočasné zablokovanie prístupu;
c) trvalé zablokovanie prístupu.

3.23. Po zistení priestupku zvolí lokálny správca IKT stupeň obmedzenia prístupu podľa závažnosti priestupku. V nejasných prípadoch môže správca okamžite zablokovať prístup k sieti UMB až do momentu vyjasnenia situácie (posúdenie motívov konania používateľa, zistenie následkov konania používateľa, rozsahu škôd a pod.). Následné rozhodnutie o stupni obmedzenia prístupu schvaľuje vedenie UAKOM-u na základe návrhu príslušného správcu. Pri rozhodnutí o stupni obmedzenia prístupu k sieti UMB môže byť zohľadnené pracovné zaradenie zamestnanca resp. študijný odbor študenta tak, aby nedošlo k znemožneniu plnenia pracovných resp. študijných povinností používateľa MS.

3.24. Porušenie ustanovení tejto smernice bude u zamestnancov UMB kvalifikované ako porušenie pracovných povinností a bude posudzované v zmysle Zákonníka práce, Pracovného poriadku UMB a nadväzných predpisov. Porušenie ustanovení tejto smernice u študentov bude kvalifikované ako porušenie študijných povinností vyplývajúcich zo zák.č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Študijného poriadku UMB a ďalších . Týmto nie je vylúčený ďalší postih vyplývajúci z porušenia ďalších zákonov či ustanovení.

3.25. V prípade, že v dôsledku neoprávneného alebo nedbanlivého konania používateľa MS vznikne materiálna škoda na sieťových prvkoch MS UMB alebo iné náklady potrebné na odstránenie problému zavineného týmto používateľom, je tento používateľ MS povinný tieto škody resp. náklady uhradiť.

## Článok 4
## Prístup používateľov do MS UMB

4.1. Zamestnanci UMB sa môžu pripájať do MS UMB na svojom pracovisku prostredníctvom káblového pripojenia a vybudovanej štruktúrovanej kabeláže. V lokalitách, ktoré sú pokryté signálom bezdrôtovej (WiFi) siete UMB, sa môžu pripájať do siete s názvom (SSID) „UMB-staff", „eduroam" a „UMB-guest".

4.2. Študenti UMB sa môžu pripájať do MS UMB prostredníctvom káblového pripojenia vo vyhradených priestoroch fakúlt (počítačové učebne, samoobslužné terminály na chodbách, prípojné miesta – vyhradené sieťové zásuvky), podľa technických a ekonomických možností fakúlt a na základe povolenia udeleného vedením fakulty. Pri práci v počítačových učebniach sú študenti v prípade vyzvania povinní preukázať sa platným preukazom študenta UMB. V lokalitách, ktoré sú pokryté signálom bezdrôtovej (WiFi) siete UMB, sa môžu pripájať do siete s názvom (SSID) „eduroam" a „UMB-guest".

4.3. Študenti a zamestnanci UMB ubytovaní na internátoch - Študentských domovoch (ďalej len „ŠD") riadených Správou účelových zariadení UMB (ďalej len „SÚZ UMB") sa môžu pripájať do MS UMB prostredníctvom káblového pripojenia v tých izbách, kde je nainštalovaná zásuvka pre pripojenie do siete. Ubytovaním sa na izbe ŠD nevzniká ubytovanému automaticky nárok na pripojenie do siete. Za materiálnu stránku pripojenia do siete na ŠD (sieťové zásuvky, kabeláže) zodpovedá SÚZ UMB. Riešenie funkčných problémov spojených s pripájaním používateľov MS do siete na ŠD zabezpečuje UAKOM, v rámci dostupných riešiteľských kapacít, bez garancie okamžitej odozvy na požiadavky používateľov MS. Podpora zo strany UAKOM sa nevzťahuje na problémy súvisiace s prevádzkovaním samotných koncových zariadení používateľov MS (napr. odstraňovanie vírusových nákaz, problémy so spúšťaním aplikácií alebo funkčnosťou operačného systému,

hardvérové problémy a pod.). Požiadavky na podporu študenti adresujú na Helpdesk UMB, e-mailový kontakt helpdesk@umb.sk, primárne zo svojej študentskej mailovej schránky.

4.4. UMB v snahe zabezpečiť možnosť pripojenia do Internetu aj pre osoby, ktoré nie sú zamestnancami, študentami alebo oficiálnymi hosťami UMB (stážisti, lektori), zriadila alternatívne sieťové pripojenie do Internetu prostredníctvom komerčného operátora. Takéto pripojenie je dostupné vo forme káblového pripojenia vo vyhradených hosťovských izbách v ŠD. Ubytovaním sa na hosťovskej izbe ŠD nevzniká ubytovanému automaticky nárok na pripojenie do siete a na garantovanú šírku prenosového pásma a kvalitu pripojenia. Ubytovaná osoba na hosťovskej izbe si nemôže nárokovať dostupnosť a funkčnosť služieb v sieti internet v konkrétnom čase. Pre materiálnu stránku pripojenia a riešenie funkčných problémov platí znenie uvedené v bode 4.3.

4.5. Subjekty, ktoré nie sú organizačnými zložkami UMB, ale majú od UMB prenajaté priestory na realizáciu svojich aktivít, môžu požiadať o sieťové pripojenie do Internetu prostredníctvom komerčného operátora v prípade, že v prenajatých priestoroch je vybudovaná káblová infraštruktúra. Prenajatím priestorov nevzniká nájomcovi automaticky nárok na pripojenie do siete. Za materiálnu stránku pripojenia do siete zodpovedá príslušná organizačná zložka UMB (fakulta, celouniverzitné pracovisko), ktorá spravuje príslušné priestory. Pre riešenie funkčných problémov platí znenie uvedené v bode 4.3.

4.6. Pre podujatia, organizované v priestoroch UMB (konferencie, semináre, školenia, propagačné akcie) je možné na základe žiadosti sprístupniť pre účastníkov akcie pripojenie do bezdrôtovej (WiFi) siete s názvom (SSID) „UMB-conference" alebo „UMB-event". Žiadosť o vytvorenie takéhoto prístupu (príloha 04.6) je potrebné doručiť na UAKOM minimálne 3 pracovné dni pred začiatkom podujatia, pričom musí obsahovať údaje:

a) názov a účel podujatia,
b) miesto a čas konania podujatia,
c) predpokladaný počet účastníkov,
d) kontaktná osoba.

4.7. Správca MS UMB nie je povinný zrealizovať také požadované zmeny v rámci MS UMB, ktoré ohrozujú bezpečnosť alebo prevádzku MS alebo nie sú dostupné informácie na základe ktorých je možné vyhodnotiť dopady.

## Článok 5
## Kontá používateľov MS v IT systémoch UMB

5.1. Prístup do väčšiny IT systémov UMB vyžaduje autentifikáciu používateľov MS.

5.2. Každý zamestnanec alebo študent UMB má pri svojom nástupe vytvorené tzv. konto UMB. Toto konto slúži na prihlasovanie sa do IT systémov UMB, ktorých zoznam je uvedený na webovej stránke https://helpdesk.umb.sk.

5.3. Okrem konta UMB môže mať používateľ MS pridelené ďalšie kontá, ktoré potrebuje pre svoju prácu alebo štúdium (napríklad konto v Akademickom informačnom systéme atď.).

5.4. Každé konto používateľa MS je chránené proti zneužitiu heslom, ktoré je povinný držať v tajnosti.

5.5. Používateľ MS UMB (ďalej len „používateľ") musí dodržiavať nasledovné podmienky:

5.5.1. Používateľ sa smie v systémoch UMB autentifikovať len kontami, ktoré mu boli pridelené.

5.5.2. Používateľ musí dbať na utajenie svojich prihlasovacích údajov a nesmie sprístupniť svoje konto ďalšej osobe.

5.5.3. Používateľ nesmie zadať prihlasovacie údaje konta UMB do systémov, ktoré nie sú v správe UMB (napríklad webové stránky, ktorých doménové meno nekončí znakmi „umb.sk") alebo ich prevádzkovateľ nemá s UMB zmluvný vzťah. Zoznam systémov, ktoré UMB nemá v správe a je v nich dovolené používať prihlasovacie údaje konta UMB je uvedený na webovej stránke https://helpdesk.umb.sk.

5.5.4. Pri vytvorení konta používateľa sa zároveň automaticky vygeneruje prístupové heslo. Používateľ je povinný si toto heslo zmeniť po prvom prihlásení do siete a nové heslo

uchovávať v tajnosti (nie je prípustné zaznamenať si heslo na mieste alebo médiu ľahko prístupnom iným používateľom). Heslo nesmie byť totožné resp. podobné s menom alebo priezviskom používateľa alebo so slovom uvedeným v slovníku (slovenskom aj inojazyčnom). Heslo nesmie obsahovať znaky s diakritikou. Dĺžka hesla musí byť minimálne 8 znakov a musí byť tvorené kombináciou aspoň 3 typov znakov z nasledovných skupín:

- veľké písmená;
- malé písmená;
- číslice;
- ostatné znaky na klávesnici (!#$&*,./ ...).

5.5.5. Používateľ je povinný meniť si svoje heslo ku kontu UMB najmenej každých 180 dní.

5.6. Prístup externých dodávateľov do IT systémov UMB musí spĺňať nasledovné podmienky:

5.6.1. Externí dodávatelia IT systémov alebo služieb musia pri prístupe do IT systémov UMB používať kontá, ktoré im boli vytvorené podľa postupu definovaného v bode 5.3.

5.6.2. Kontá pre dodávateľov je možné vytvárať len na základe existencie zmluvného vzťahu a to len na dobu trvania kontraktu.

5.6.3. Pokiaľ je to možné, odporúča sa vytvárať kontá viazané priamo na osoby, ktoré objednané služby vykonávajú a zodpovedajú za utajenie poskytnutých prístupových informácií.

5.7. Životný cyklus kont zamestnancov a študentov UMB a ich správu zabezpečuje systém pre správu identít (IDM) na základe informácií zo systémov SAP a AIS pri dodržiavaní nasledovných zásad:

5.7.1. Kontá zamestnancov UMB sa vytvárajú automatizovane na základe dát zo zdrojového systému SAP/Sofia. Po vytvorení konta sú prihlasovacie údaje preposlané e-mailom lokálnemu správcovi IKT danej súčasti UMB, na ktorej bude zamestnanec pracovať. Ak sa konto vygenerovalo ešte pred skutočným začiatkom pracovného pomeru zamestnanca, tak bude až do jeho začiatku neaktívne.

5.7.2. Kontá pre študentov UMB sa vytvárajú automatizovane na základe dát zo systému AIS. Prvý pracovný deň od potvrdenia úplného zápisu v zdrojovom systéme AIS sa študentovi vytvorí konto v IDM a prihlasovacie údaje mu budú odoslané do AIS ako správa.

5.7.3. Životný cyklus konta UMB končí pri ukončení pracovného pomeru na UMB alebo ukončení štúdia na UMB. Po ukončení pracovného pomeru alebo štúdia sa konto používateľa MS prepne do stavu ukončovaný, tzv. "ochrannej lehoty". V tejto lehote majú používatelia MS ešte prístup k svojim emailom a dátam na sieťovom úložisku, aby si ich mohli zálohovať. Prístupy k sieti (WiFi, internet na internáte) a ďalším IT systémom UMB sú im odobrané. Ochranná lehota začína plynúť prvým kalendárnym dňom nasledujúceho mesiaca a trvá 4 mesiace. Po uplynutí tejto doby sa všetky údaje spojené s používateľským kontom vymažú.

## Článok 6
## Zálohovanie elektronických dát

6.1. Ochrana elektronických dát UMB pred poškodením alebo stratou je zabezpečovaná zálohovaním dát a zálohovaním konfigurácií IT systémov. Uskutočňuje sa formou zálohovania centrálnych IT systémov a zálohovaním pracovných staníc používateľov MS.

6.2. Zálohovanie centrálnych IT systémov sa riadi týmito pravidlami:

6.2.1. Zálohujú sa len IT systémy, ktoré sú potrebné pre zabezpečovanie základných procesov UMB.

6.2.2. Každý správca IT systému je povinný v spolupráci so správcom zálohovacieho systému:

- Zabezpečiť pravidelné zálohovanie zvereného IT systému s ohľadom na špecifické potreby jeho používateľov a technické možnosti UMB;
- vypracovať plán zálohovania podľa prílohy č. 06.2a. Vypracovaný plán zálohovania musí správca IT systému odovzdať správcovi zálohovacieho systému minimálne dva pracovné dni pred dátumom plánovaného začiatku zálohovania;

- zabezpečiť aby boli súčasťou zálohy všetky dáta, konfiguračné záznamy a ďalšie údaje, ktoré sú potrebné pre jeho úplné obnovenie po strate dát alebo prístupu k jeho úložisku;
- zabezpečiť realizáciu úplného testu obnovy zvereného IT systému minimálne raz ročne. Výsledok testu obnovy zaznamená do protokolu podľa prílohy 06.2b. V prípade, že je zálohovaný IT systém v úplnej alebo čiastočnej správe externého dodávateľa, môže byť úplný test obnovy nahradený testom obnovy zálohovaných dát a potvrdením od dodávateľa, že zálohované dáta postačujú na úplnú obnovu systému. Následne správca systému odovzdá výsledok testu správcovi zálohovacieho systému;
- zabezpečiť fyzické uloženie zálohy mimo úložiska zálohovaného systému a musí byť dostupná nezávisle od stavu hardvéru alebo softvéru, na ktorom je prevádzkovaný zálohovaný systém;
- zabezpečiť šifrovanie záloh obsahujúcich autorizačné informácie;
- zabezpečiť zálohovanie všetkých programov alebo skriptov, ktoré boli vytvorené alebo modifikované špeciálne pre potreby UMB.

6.2.3. Zálohovanie dát používateľov MS uložených v ich pracovných staniciach sa riadi týmito pravidlami:

□používateľské dáta uložené v chránených pracovných staniciach musia byť zálohované;
□za zálohovanie dát vo svojej pracovnej stanici zodpovedá sám používateľ MS UMB;
□záloha dát musí byť fyzicky oddelená od pracovnej stanice a pracovná stanica nesmie mať možnosť zálohu zmazať alebo modifikovať (napríklad cez sieťové pripojenie alebo cez USB na pripojený externý disk;
□optimálny spôsob a rozsah zálohovania dát v pracovnej stanici môže používateľ MS UMB konzultovať so svojím správcom IKT;
□pracovné stanice zaradené do domény UMB majú sprístupnené sieťové úložisko označené ako disk S. Obsah tohto úložiska je zálohovaný automaticky každý deň o 18:00. Zálohy sú uchovávané po dobu 60 dní. Dáta používateľa MS UMB uložené na tomto úložisku sú považované za zálohované a nie je potrebné ich zálohovať inými metódami;
□dokumenty vytvorené kancelárskym balíkom MS Office (Word a Excel) uložené v adresároch, ktoré sú automaticky synchronizované s intranetovým portálom (intranet.umb.sk) sú považované za zálohované a nie je potrebné ich zálohovať inými metódami;
□médiá obsahujúce zálohy dát nesmú opustiť priestory univerzity;
□pracovné stanice v učebniach a dáta študentov nie sú zálohované.

## Článok 7
## Šifrovanie dát

7.1. Chránené dáta na zariadeniach, ktoré opúšťajú priestory UMB alebo hrozí zvýšené riziko ich straty alebo odcudzenia v priestoroch UMB (napr. notebooky, USB flash disky atď.) musia byť chránené šifrovaním. Zoznam schválených nástrojov na šifrovanie úložísk dát je na webovej stránke https://helpdesk.umb.sk.

7.2. Povinnosť šifrovania sa netýka pamäťových médií, ktoré neobsahujú chránené dáta.

7.3. Za zrealizovanie ochrany zariadenia, ktorého dáta majú byť podľa tejto smernice chránené šifrovaním, je zodpovedný používateľ MS UMB v spolupráci so svojím správcom IKT.

7.4. Obsah prenosných médií (USB flash disky, pevné externé disky, pamäťové karty, atď.) musí byť zabezpečený šifrovaním.

7.5. Pevné disky prenosných chránených pracovných staníc musia byť zabezpečené šifrovaním

7.6. Mobilné telefóny (inteligentné telefóny) a tablety, ktoré obsahujú chránené údaje musia byť zabezpečené šifrovaním. Zašifrované sú osobné kontá, nastavenia, aplikácie a ich dáta, média a ostatné súbory. Dáta na externej pamäťovej karte rozširujúcej úložný priestor zariadenia musia byť tiež šifrované.

7.7. Obsah pevných diskov chránených pracovných staníc, ktoré nie je možné pred odovzdaním stanice do servisu zo stanice vybrať, musí byť chránený šifrovaním.

## Článok 8
## Mazanie dát zo serverov

8.1. Osoba zodpovedajúca za obsah údajov uložených na konkrétnom serveri (ďalej len „osoba zodpovedajúca za údaje") môže požiadať UAKOM o výmaz dát zo servera a príslušnej infraštruktúry (najmä v súvislosti s ochranou osobných údajov). Vyplnenú žiadosť o výmaz dát zo servera a príslušnej infraštruktúry (príloha 08.1) zašle osoba zodpovedajúca za údaje IT bezpečnostnému správcovi UMB.

8.2. Osoba zodpovedajúca za údaje zaslaním tejto žiadosti berie na vedomie, že údaje môžu mať súvis aj s inými systémami a je si vedomá týchto súvislostí. Ďalej deklaruje, že výmaz týchto údajov nebude mať vplyv na chod ostatných systémov a výmaz je v súlade s predpismi a platnou legislatívou SR a EÚ, zaväzujúcou UMB, vrátane vnútorných predpisov UMB (napríklad povinnosť archivovať údaje po určitú dobu).

8.3. Pracovník UAKOM-u, zodpovedný za výmaz dát, nepreberá zodpovednosť za prípadné následky a škody súvisiace s výmazom týchto dát, a to aj v prípade, že nebude možná ich prípadná obnova.

8.4. Pracovník UAKOM-u následne s osobou zodpovedajúcou za údaje dohodne termín výmazu dát, spôsob a rozsah mazania.

8.5. Na požiadanie pracovník UAKOM-u zabezpečí, aby boli údaje vymazané v súlade s technickými požiadavkami definovanými v súvislosti s pravidlami ochrany osobných údajov (nenávratný výmaz a pod.).

8.6. Pri príprave a realizácii výmazu môže vzniknúť situácia, ktorá bude vyžadovať súčinnosť dodávateľa aplikácie alebo zariadenia, ktorú zabezpečí osoba zodpovedajúca za údaje.

8.7. Osoba zodpovedajúca za chod konkrétneho servera je povinná poskytnúť súčinnosť pracovníkom UAKOM-u a v prípade potreby aj oslovenému dodávateľovi, vo všetkých fázach prípravy a realizácie.

## Článok 9
## Pravidlá používania a správy pracovných staníc

9.1. Inštalácia softwarového vybavenia je v kompetencii lokálneho správcu IKT príslušného k jednotlivej súčasti UMB.

9.2. Pracovné stanice UMB je možné používať jedine na pracovné účely, teda sa zakazuje používať pracovné stanice na súkromné účely, vrátane spracovávania súkromných dát akoukoľvek formou. V prípade študentov sa činnosti priamo súvisiace so štúdiom pre potreby tejto smernice v tomto bode chápu ako pracovné účely.

9.3. Pre zabezpečenie ochrany koncových pracovných staníc je potrebné dodržať nasledovné úkony:

a) Inštalácia bezpečnostných záplat;
b) Inštalácia a aktualizácia antivírového softvéru;
c) Vynucovanie komplexnosti hesla minimálne na úrovni definovanej článkom 5 tejto smernice.

9.3.1. Používateľ pracovnej stanice nesmie:

- mať administrátorské oprávnenia na úrovni operačného systému;
- odmietnuť aktualizáciu operačného systému;
- meniť, vypínať alebo inak zasahovať do chodu antivírového softvéru;

- inštalovať alebo používať neschválený softvér;
- meniť systémové nastavenia;
- používať lokálne konto;
- inak svojou činnosťou ohrozovať, obmedzovať alebo znemožňovať výkon akýkoľvek úkonov vykonávaných za účelom zvyšovania bezpečnosti spracovávaných údajov, software, a samotného zariadenia.

9.3.2. Pracovná stanica musí mať vypnuté automatické spúšťanie programov z externých dátových médií (autorun).

9.3.3. Pracovná stanica musí mať nastavené automatické zamknutie operačného systému po uplynutí najviac 15 minút nečinnosti. V prípade, že sa jedná o notebooky aj pri zatvorení displeja.

9.3.4. Pracovná stanica nesmie zároveň slúžiť ako server pre iných používateľov MS.

9.3.5. Používateľ MS je pri krátkodobej neprítomnosti povinný inicializovať zamknutie operačného systému (napr. stlačením Win+L (platné pre systémy Windows)).

9.3.6. Pracovná stanica musí byť zaradená do domény UMB. V prípade, že pracovnú stanicu nie je technicky možné zaradiť do domény UMB, správca IKT je povinný zabezpečiť ochranu zariadenia a dát na koncovom zariadení minimálne v rozsahu definovanom v Bezpečnostnej smernici UMB (najmä v bode 4).

9.3.7. Správca IKT je povinný zabezpečiť aby sa na pracovných staniciach používali len aktuálne a aktualizované verzie softvérového vybavenia (najmä operačný systém a internetový prehliadač) a používal sa len softvér, ktorý má aktívnu podporu od výrobcu. V odôvodnenom prípade môže IT bezpečnostný správca udeliť výnimku.

9.4. V prípade, že sa pracovná stanica používa na účely spracovávania osobných údajov jedná sa o chránenú pracovnú stanicu.

9.4.1. Koncový používateľ je povinný bezodkladne upovedomiť príslušného správcu IKT o skutočnosti, že sa jedná o chránenú pracovnú stanicu.

9.4.2. Lokálny správca je povinný pri administrácii chránenej pracovnej stanice postupovať v súlade s Bezpečnostnou smernicou UMB (jedná sa hlavne, no nie len, o body 4.6.5 až 4.6.10 Bezpečnostnej smernice UMB).

9.4.3. V prípade, že sa jedná o pracovnú stanicu definovanú ako chránená pracovná stanica musí mať navyše oproti bodu 9.3 aplikované nasledovné bezpečnostné opatrenia a nastavenia:

a) používateľ nesmie odmietnuť reštart, ak je potrebný pre účely aplikácie bezpečnostných záplat. Dovoľuje sa pozastaviť reštart najdlhšie však do konca pracovnej doby daného dňa;
b) používateľ nesmie používať iné ako správcom nainštalované a schválené programy;
c) v prípade, že sa jedná o mobilnú pracovnú stanicu je potrebné zamedziť prenosu údajov mimo priestory UMB (zamedziť ukladaniu dát do neschválených cloudových úložísk, prenosu na nechránených médiách, prenosu nechránených záloh na prenosných médiách, atď.);
d) v prípade potreby prenosu pracovnej stanice mimo priestorov UMB je potrebné zabezpečiť šifrovanie údajov podľa článku 7 tejto smernice;
e) o ukončení zodpovednosti za chránenú pracovnú stanicu je používateľ povinný informovať lokálneho správcu IKT. V spolupráci s lokálnym správcom IKT zabezpečiť likvidáciu chránených dát v súlade s bezpečnostným projektom a Bezpečnostnou smernicou UMB.

9.5. Správca IKT môže nastavovať výnimky z uvedených systémových nastavení, ktoré sú nevyhnutné pre chod regulárnych aplikácií. Pri udeľovaní výnimky je povinný dbať na dodržiavanie zásad definovaných v platných smerniciach UMB, najmä v tejto smernici a v Bezpečnostnej smernici UMB.

9.6. Každá pracovná stanica musí mať definovaného správcu IKT.

9.6.1. Správca pracovnej stanice je povinný viesť evidenciu údajov pre každú pracovnú stanicu. Evidencia údajov sa vedie na intranete UMB v rozsahu:

a) fyzické adresy sieťových rozhraní (MAC adresa);
b) identifikátor sieťovej zásuvky, do ktorej je počítač pripojený;
c) fyzické umiestnenie pracovnej stanice (budova, číslo miestnosti);

d) mená používateľov, ktorým bola pracovná stanica primárne priradená;
e) bezpečnostnú klasifikáciu (či sa jedná o chránenú pracovnú stanicu);
f) zoznam výnimiek z uvedených systémových nastavení udelených správcom.

9.6.2. Správca môže za účelom administrácie pristupovať na akúkoľvek pracovnú stanicu, ktorú spravuje. V prípade, že je to možné, správca je povinný informovať o tejto skutočnosti koncového používateľa, ktorému bola pracovná stanica primárne priradená.

9.6.3. Koncový používateľ nesmie akýmkoľvek spôsobom brániť správcovi vo výkone činností súvisiacich s administráciou pracovnej stanice.

9.7. V prípade, že lokálny správca IKT narazí na problém alebo úlohu, ktorá nie je riešiteľná v jeho možnostiach alebo kompetenciách a súčasne je pre vyriešenie problému alebo úlohy potrebná súčinnosť pracovníkov UAKOM-u, je lokálny správca IKT povinný nahlásiť požiadavku cez helpdeskový systém Redmine. V opačnom prípade sa pracovníci UAKOM-u nebudú touto požiadavkou zaoberať.

## Článok 10
## Prístup k dátam a do pracovných staníc UMB

10.1. Fyzický prístup do pracovných staníc majú:
- používatelia MS UMB s kontom v doméne UMB, alebo v doméne STUDENTI na úrovni oprávnený používateľ;
- lokálni správcovia IKT pristupujúci cez lokálne administrátorské kontá alebo doménové kontá s administrátorskými oprávneniami;
- vybraní pracovníci UAKOM pristupujúci cez doménové kontá.

10.2. Vzdialený prístup do pracovných staníc používateľov MS UMB je možný len so súhlasom správcu MS UMB. V odôvodnených prípadoch môže používateľ MS UMB získať vzdialený prístup do pracovnej stanice, ktorá mu bola pridelená zaslaním vyplnenej žiadosti o umožnenie vzdialeného prístupu (príloha 10.2) e-mailom na adresu helpdesk@umb.sk . Každá žiadosť bude posudzovaná individuálne. O schválení alebo neschválení žiadosti a ďalšom postupe bude používateľ MS informovaný e-mailom. V prípade, že žiadosť bude vyhodnotená kladne, prístup bude umožnený najskôr do troch pracovných dní od schválenia žiadosti.

10.3. V prípade, že pre potreby UMB je nevyhnutné sprístupniť pracovné dáta používateľa MS, uložené na jemu pridelenej pracovnej stanici alebo v serverových aplikáciách a cloudových úložiskách, je možné tak vykonať za podmienok:

10.3.1. Lokálny správca IKT môže pristupovať na pracovnú stanicu používateľa MS jedine na základe žiadosti nadriadeného pracovníka dotknutého používateľa MS (príloha 10.3). Táto žiadosť musí byť lokálnemu správcovi IKT doručená buď písomnou formou alebo elektronicky zaslaním e-mailu na adresu helpdesk@umb.sk, kde bude zaznamenaná v helpdeskovom systéme. Lokálny správca IKT následne sprístupní údaje nadriadenému pracovníkovi dotknutého používateľa MS.

10.3.2. V prípade, že pre potreby UMB je nevyhnutné sprístupniť dáta používateľa MS UMB v serverových aplikáciách a cloudových úložiskách, na ktoré lokálny správca IKT nemá dosah, na základe žiadosti nadriadeného pracovníka dotknutého používateľa (príloha 10.3) lokálny správca IKT požiada UAKOM o sprístupnenie týchto údajov. Žiadosť musí byť zaznamenaná v helpdeskovom systéme REDMINE. Lokálny správca IKT následne sprístupní údaje nadriadenému pracovníkovi dotknutého používateľa MS UMB.

10.3.3. Tento postup nie je možné aplikovať na sprístupnenie údajov nachádzajúcich sa v mailovej schránke používateľa. V takom prípade je potrebné postupovať podľa bodu 12.14.

## Článok 11
## Popis Metropolitnej siete UMB, jej ochrana, obnova a rozvoj, procesy obstarávania nových prvkov a súčastí

11.1. Komunikačná infraštruktúra Metropolitnej siete UMB pozostáva z množiny prvkov troch kategórií:

- **Pasívne siete**
  a) metropolitná optická sieť (MOS UMB-NET) na úrovni mesta, prenosovým médiom je jednovidové optické vlákno (SMF);
  b) lokálne optické kabeláže prepájajúce budovy alebo ich časti v rámci jednej lokality, prenosovým médiom je jednovidové (SMF) alebo gradientné (MMF) optické vlákno;
  c) lokálne metalické kabeláže (štruktúrovaná kabeláž) prepájajúce komunikačné uzly s prakticky všetkými miestnosťami budov fakúlt a internátov, prenosovým médiom je krútená dvojlinka z izolovaného CU drôtu (TP) ;
  d) pasívnou sieťou pre bezdrôtové pripojenie (rádiové, WiFi) je voľný priestor.
- **Aktívne komunikačné prvky – smerovače, prepínače** (centrálne, agregačné, prístupové);
- **Aktívne prvky bezdrôtových sietí (WiFi)** – pozostávajú z prístupových bodov (AP), určených na pripájanie mobilných zariadení, sú na hierarchickej úrovni prístupového prepínača.

Prepojenie potrebného počtu prvkov týchto kategórií, zohľadňujúce geografické a organizačné členenie UMB v meste BB, tvorí topológiu siete. Topológia je formálne definovaná prepojovacím plánom.

11.2. Koncové zariadenia MS UMB rozdeľujeme do štyroch kategórií:

- **Koncové zariadenia typu počítač** - napr. stolný počítač, prenosný počítač, priemyselný počítač, smartfón, tablet, atď.
- **Koncové zariadenia na tvorbu a interpretáciu číslicového multimediálneho obsahu** - napr. kamera (fotoaparát), monitor, televízor, telefón, audio zariadenia pre nahrávanie a/alebo reprodukciu zvuku, atď.
- **Koncové zariadenia serverovej infraštruktúry** - napr. servery (HW rôzneho prevedenia), úložiská údajov, diskové polia, sieťové disky, sieťové tlačiarne a/alebo tlačové servery, atď.
- **Ostatné (koncové) zariadenia** - ktoré môžu a nemusia byť pripojené do dátovej siete, ale majú priamy alebo nepriamy vplyv na spoľahlivú prevádzku a funkčnosť zariadení z predchádzajúcich kategórií, napr. zdroje nepretržitého napájania, motorgenerátory, klimatizačné zariadenia, chladiče, elektrické rozvádzače a rozvodne, atď.

11.3. Prevádzkovateľom všetkých centrálnych IT systémov, komunikačnej infraštruktúry a zariadení je UAKOM, ktorý je aj hlavným konzultantom pri akejkoľvek požiadavke na ich rozšírenie. Medzi centrálne IT systémy patria aj dochádzkový a prístupový IT systém, stravovací IT systém, energetický IT systém alebo IT systém telefonickej prevádzky.

11.4. Náklady na budovanie komunikačnej infraštruktúry sú vysoké, ale aj jej morálna a fyzická životnosť je vysoká. To znamená, že pri poškodení alebo zničení časti infraštruktúry vzniknú organizácii (UMB) veľké škody. V nasledujúcich odsekoch sú vymenované reálne hrozby a riziká poškodenia pre jednotlivé prvky MS UMB a spôsoby ako ich znížiť alebo úplne eliminovať.

11.4.1. **Pasívne siete** - MOS UMB-NET v intraviláne mesta pozostáva z optických káblov zakopaných v zemi. Hrozí tu riziko poškodenia pri prípadnej stavebnej činnosti (zemné práce), ak neboli dodržané zákonné postupy alebo termíny pri stavebnom konaní. Riziko poškodenia hrozí aj pri odstraňovaní havárie na vodovodnom alebo plynovom potrubí alebo na elektrickom VN kábli. Podobné riziko hrozí aj pre lokálne optické kabeláže prepájajúce budovy alebo ich časti v rámci jednej lokality, pokiaľ sú zakopané v zemi.

11.4.2. **Lokálne metalické kabeláže** (štruktúrovaná kabeláž) - prepájajúce komunikačné uzly s prakticky všetkými miestnosťami budov fakúlt a internátov. Hrozí tu riziko náhodného poškodenia káblov pri drobných stavebných úpravách a opravách, ďalej riziko znefunkčnenia dátových zásuviek pri maľovaní stien. Na internátnych izbách je

permanentné riziko zničenia dátových zásuviek a to buď zámerného, z nedbalosti alebo náhodného.

11.4.3. **Aktívne komunikačné prvky pre káblové pripojenie** - sú bez rizík odcudzenia, požiaru alebo poškodenia. Tie boli eliminované už pri budovaní komunikačných uzlov.

11.4.4. **Aktívne prvky bezdrôtových sietí** – prístupové body. Hrozí minimálne riziko poškodenia z hrubej nedbalosti pri stavebných a montážnych prácach a minimálne riziko odcudzenia. Minimalizovanie týchto rizík bolo vykonané už pri inštalácii prístupových bodov.

11.4.5. **Koncové zariadenia typu počítač a multimediálne koncové zariadenia** - keďže sú hnuteľné a vypínateľné, nehrozí riziko poškodenia pri akýchkoľvek prácach. Avšak je tu isté riziko odcudzenia. Ťarchu tohto rizika znáša osoba zapísaná na karte majetku príslušného zariadenia.

11.4.6. **Koncové zariadenia serverovej infraštruktúry a ostatné zariadenia** - sú bez rizík odcudzenia, požiaru alebo poškodenia. Tie boli eliminované už pri budovaní komunikačných uzlov a serverovní.

11.4.7. Na základe analýzy a rozboru rizík podľa odsekov 11.4.1. až 11.4.6. **pracovisko UAKOM musí byť informované o každej plánovanej (vopred) aj neplánovanej (bezodkladne) stavebnej činnosti na ktoromkoľvek pozemku a/alebo budove UMB.** Pracovníci UAKOM potom zhodnotia konkrétnu hrozbu vzniku škody na majetku MS UMB a navrhnú opatrenia na elimináciu tejto hrozby. Informáciu musí odoslať (s požiadavkou na spätné potvrdenie) príslušný referát správy budov.

11.5. Všetky prvky MS UMB podľa popisu v bodoch 11.1. a 11.2., ktoré sú prepojené musia byť navzájom kompatibilné. To znamená, že v styčných bodoch musia podporovať rovnaké štandardy (pokiaľ sú definované) a musia byť parametrovo a výkonovo prispôsobené. Obnovu a rozvoj komunikačnej infraštruktúry takmer výhradne zabezpečuje UAKOM. S cieľom vyhnúť sa prípadnej nekompatibilite (následnej nepoužiteľnosti) jednotlivých prvkov MOS UMB-NET, je potrebné pri obstaraní dodržať nasledovný postup:

11.5.1. **Prípravná fáza** - organizačná súčasť UMB, ktorá plánuje obstarať prvky z vyššie uvedených kategórií alebo pripravuje projekt na realizáciu určitého funkčného celku, ktorého súčasťou budú tieto prvky, je povinná konzultovať svoje návrhy s vybranými pracovníkmi UAKOM už v čase prípravy investičnej akcie/projektu/nákupu. V rámci konzultácie sa tiež definuje, aké služby budú požadované od UAKOM v súvislosti s pripravovaným zámerom (také, ktoré nemôže/nesmie /nemá zabezpečiť dodávateľ z rôznych dôvodov (bezpečnosť) a pod.).

11.5.2. **Predrealizačná fáza** - začína okamihom, keď je už známy dodávateľ a predmet dodávky (konkrétne a podrobne). Ak ide o realizáciu zložitejšieho zámeru, je nevyhnutné konzultovať s UAKOMom aj postup realizácie. Niektoré činnosti je možné a vhodné uskutočniť ešte pred samotnou realizáciou (napr. konfigurácia, predkonfigurácia zariadení, prípadne funkčná skúška, a pod. V takomto prípade zadávateľ (súčasť UMB) je pri plánovaní povinný prihliadať, na základe konzultácie s definovanými pracovníkmi UAKOM, na aktuálnu alokáciu zdrojov UAKOMu v momente spustenia predrealizačnej fázy. Štandardne sa počíta rozsahom minimálne 3 – 5 pracovných dní, potrebných na technické úkony realizované UAKOMom.

11.5.3. **Realizačná fáza** - pri väčšej dodávke, ktorej realizácia bude trvať viac dní (až týždne), je potrebné zabezpečiť stály dohľad nad prácou dodávateľa z dôvodu bezpečnosti a ochrany majetku a osôb. UAKOM, pokiaľ nie je na realizácii priamo zainteresovaný, si robí iba vlastný monitoring priebehu, prípadne poskytuje vopred dohodnuté služby. Za dohľad je zodpovedná príslušná organizačná jednotka UMB. Dohľad vykonáva poverená osoba. Dohľad v komunikačnom uzle musí vykonávať odborne spôsobilá osoba, čiže príslušný správca IKT alebo pracovník UAKOM, ak je to nevyhnutné.

11.6. Postupy uvedené v bode 11.5. tejto smernice je nutné dodržiavať pri nákupe akejkoľvek časti IT systému. Za IT systémy sa považujú aj prístupové systémy (otváranie dverí alebo rampy), čítačky kariet, monitoring energetiky a tepelného hospodárstva.

## Článok 12
## Mailový systém

12.1. Mailový systém umožňuje zamestnancom UMB prostredníctvom e-mailovej schránky prijímanie a odosielanie elektronickej pošty v rámci celej siete internet. Každý zamestnanec UMB je povinný používať na pracovnú komunikáciu výhradne e-mailovú adresu, ktorá mu bola pridelená podľa tohto článku. Každý študent UMB je povinný na komunikáciu so zamestnancami UMB používať výhradne mailovú adresu, ktorá mu bola pridelená podľa tohto článku. Pridelenú mailovú schránku smie zamestnanec využívať výhradne na pracovné účely. Používanie mailovej schránky zamestnanca na súkromné účely je zakázané. Ak zamestnanec prijme do pracovnej mailovej schránky správu súkromnej povahy je povinný ju bezodkladne vymazať.

12.2. Prijímanie a odosielanie elektronickej pošty je zabezpečované s využitím cloudovej služby Office 365 prevádzkovanej spoločnosťou Microsoft. Okrem služby elektronickej pošty (e-mail) používateľ MS môže využívať na elektronickú komunikáciu aj ďalšie produkty z balíka Office 365, ktoré sú dostupné na základe jemu pridelenej licencie. Informácie o kapacite mailovej schránky a jej ďalšie parametre sú dostupné na portáli https://helpdesk.umb.sk.

12.3. Odporúčanou metódou práce s mailovou schránkou na pracovnej stanici zamestnanca je používanie poštového klienta Microsoft Outlook, ktorý je súčasťou balíka Microsoft Office. Okrem poštového klienta Microsoft Outlook je možné pre prístup k pošte použiť webové rozhranie poštového klienta, ktoré je dostupné na adrese https://outlook.office.com. Tento prístup je možný z ktoréhokoľvek počítača pripojeného k internetu. Do webového rozhrania je dovolené sa prihlasovať len z dôveryhodných počítačov.

12.4. Okrem spôsobov opísaných v bodoch 12.2. a 12.3. je možné použiť aj alternatívnych poštových klientov. Alternatívny poštový klient musí podporovať protokoly SMTP, IMAP alebo POP3 so zabezpečením SSL/TLS. Prístup do mailovej schránky cez nezabezpečené spojenie (bez SSL/TLS) sa zakazuje. Nastavenie protokolov SMTP, IMAP alebo POP3 pre poštových klientov sa nachádza na webovej stránke https://helpdesk.umb.sk. V prípade použitia iných spôsobov prístupu ako sú opísané v bodoch 12.2. a 12.3. zodpovedá za ich konfiguráciu a riešenie prípadných problémov sám používateľ MS.

12.5. Každému zamestnancovi alebo študentovi UMB je pridelená jedna mailová adresa. Mailová adresa používateľa MS UMB sa skladá z dvoch častí:

- Identifikátor používateľa v tvare *meno.priezvisko*;
- Doména používateľa v tvare *umb.sk* alebo *studenti.umb.sk*.

12.6. Ak je zamestnanec zároveň aj študentom UMB, má právo na pridelenie dvoch mailových adries, a to jednej s doménou umb.sk a druhej s doménou studenti.umb.sk. V prípade, že má daný používateľ MS UMB mailovú adresu v doméne umb.sk rovnako aj v doméne studenti.umb.sk, nemusia mať tieto mailové adresy rovnaký identifikátor používateľa. Identifikátor sa môže líšiť v poradovom čísle. Názov domény používateľa MS sa riadi nasledujúcimi pravidlami:

- Zamestnanci UMB a interní doktorandi majú pridelenú doménu umb.sk;
- Študenti a externí doktorandi majú pridelenú doménu studenti.umb.sk.

12.7. Identifikátor používateľa MS je prideľovaný automatizovaným systémom a riadi sa nasledujúcimi pravidlami:

12.7.1. Identifikátor obsahuje len znaky malej abecedy bez diakritiky, bodky a číslice. Znaky s diakritikou sú konvertované na zodpovedajúce znaky bez diakritiky.

12.7.2. Identifikátor je generovaný na základe krstného mena a priezviska používateľa. Krstné meno a priezvisko sú navzájom oddelené bodkou. V prípade, že takto vytvorený identifikátor pre danú doménu je už obsadený, systém doplní za identifikátor poradové číslo, počnúc číslom 2, a znovu skontroluje jeho jedinečnosť.

12.7.3. V prípade, že dôjde k zmene mena alebo priezviska používateľa MS v systéme Sofia alebo systéme AIS2 systém automaticky vytvorí pre používateľa MS novú mailovú adresu podľa

vyššie uvedených pravidiel . Po vytvorení novej mailovej adresy bude do poštovej schránky doručovaná aj pošta odosielaná na pôvodnú mailovú adresu.

12.8. V odôvodnených prípadoch môže používateľ MS požiadať UAKOM o zmenu svojej mailovej adresy mimo pravidiel uvedených v bode 12.4. Používateľ MS môže o zmenu e-mailovej adresy požiadať zaslaním správne vyplnenej žiadosti o zmenu mailovej adresy (príloha 12.8) v prílohe e-mailu zaslaného na adresu helpdesk@umb.sk. Požadovaný tvar novej e-mailovej adresy musí korešpondovať s pravidlami vytvárania e-mailových adries, definovaných v bode 12.5. Čas potrebný na preverenie žiadosti, vyjadrenie a realizáciu požadovanej zmeny je minimálne 3 pracovné dni. Zmena bude vykonaná len v prípade, že bude realizovateľná z technického hľadiska. Tvar novo pridelenej e-mailovej adresy nemusí byť totožný s požadovaným tvarom e-mailovej adresy podľa žiadosti používateľa MS. Po zmene mailovej adresy bude do poštovej schránky doručovaná aj pošta odosielaná na pôvodnú mailovú adresu.

12.9. V prípade potreby (konferencia, zber údajov, atď.) je možné požiadať o vytvorenie osobitnej mailovej schránky, ktorá nie je viazaná na konkrétnu osobu a môže do nej pristupovať alebo z nej odosielať správy viac ako jeden používateľ MS UMB. Takúto schránku vytvorí správca mailového systému na základe správne vyplnenej žiadosti, príloha č. 12.9.

12.10. Za archiváciu správ na osobnom počítači zodpovedá každý používateľ MS UMB sám. V prípade problémov alebo nejasností môže požiadať o pomoc lokálneho správcu IKT.

12.11. Po ukončení pracovného pomeru alebo štúdia je obsah mailovej schránky pre používateľa MS dostupný ešte po dobu štyroch kalendárnych mesiacov. Počas tejto doby môže používateľ MS schránku používať len na čítanie správ, nemôže z nej správy odosielať.

12.12. Mailová adresa používateľa MS je rezervovaná (nie je ju možné prideliť inému používateľovi MS) po dobu piatich rokov od ukončenia pracovného pomeru zamestnanca alebo po dobu jedného roka od ukončenia štúdia študenta.

12.13. Študent komunikuje s pracovníkmi technickej podpory výhradne cez mailovú adresu helpdesk@umb.sk. V prípade použitia inej mailovej adresy jeho požiadavka nebude vybavená. Inú mailovú adresu môže použiť len v prípade, že sa nevie prihlásiť do pridelenej mailovej adresy na komunikáciu s pracovníkmi technickej podpory. V takomto prípade je študent povinný v e-maily uviesť nasledovné údaje:

a) meno, priezvisko;
b) AIS ID;
c) študijný odbor.

12.14. UMB ako zamestnávateľ má právo sprístupniť obsah ním zriadenej mailovej schránky zamestnanca v dvoch prípadoch:

12.14.1. Na žiadosť orgánov činných v trestnom konaní, ktoré sa riadi platnou legislatívou SR.

12.14.2. Na žiadosť nadriadeného zamestnanca a to len v prípade, že existuje dôvod sa domnievať, že v mailovej schránke zamestnanca sa nachádza správa, ktorá obsahuje informácie nutné pre vykonanie činnosti, ktorej odklad by mohlo ohroziť oprávnené záujmy zamestnávateľa a tieto údaje nie je možné v rámci organizácie získať iným spôsobom. Zároveň musí byť splnená niektorá z nasledujúcich podmienok:

a) zamestnanec odmieta spolupracovať alebo náhle ukončil pracovný pomer;
b) zamestnanec z dôvodu PN alebo z dôvodu osobných prekážok v práci nemôže pracovať s mailovou schránkou;
c) zamestnanec je na dovolenke, kde nemá prístup k mailom alebo nie je zastihnuteľný;

12.14.3. Pred sprístupnením schránky sa žiadateľ pokúsi používateľa MS kontaktovať dostupnými kanálmi a informovať ho o nahliadnutí do jeho schránky jemu nadriadeným pracovníkom.

12.14.4. Do mailovej schránky je možné nahliadnuť len po predložení správne vyplnenej žiadosti o nahliadnutie do mailovej schránky zamestnanca (príloha 12.14a), ktorej súčasťou musí byť súhlas osoby zodpovednej za spracovanie osobných údajov organizačnej jednotky, ku ktorej zamestnanec prináleží a spôsob a výsledok pokusu o kontaktovanie zamestnanca podľa bodu 12.14.3.

12.14.5. Správne vyplnenú žiadosť doručí žiadateľ IT bezpečnostnému správcovi na posúdenie. V prípade, že IT bezpečnostný správca túto žiadosť posúdi ako oprávnenú vyjadrí súhlas svojim podpisom na žiadosti.

12.14.6. IT bezpečnostný správca následne žiadosť postúpi správcovi mailového systému, ktorý kontaktuje žiadateľa a dohodne si s ním termín vykonania úkonu.

12.14.7. Na základe riadne vyplnenej žiadosti za fyzickej prítomnosti žiadateľa, správca mailového systému nahliadne do mailovej schránky dotknutého používateľa a spoločne so žiadateľom identifikujú predmetnú komunikáciu.

12.14.8. Následne správca mailového systému túto komunikáciu odovzdá žiadateľovi v digitálnej alebo tlačenej forme. Nie je dovolené posielať akékoľvek správy z mailovej schránky dotknutého používateľa (ani preposlať predmetnú komunikáciu). Zakazuje sa umožniť žiadateľovi prístup do mailovej schránky zamestnanca bez prítomnosti správcu mailového systému.

12.14.9. Po skončení úkonu vyplní správca mailového systému spolu so žiadateľom protokol o nahliadnutí do mailovej schránky (príloha 12.14b). Protokol bude vyhotovený v troch exemplároch a bude doručený nasledovným príjemcom: UAKOM, osoba zodpovedná za OOU na príslušnej organizačnej jednotke a dotknutá osoba. Doručenie protokolu zabezpečí žiadateľ.

12.15. Technickú podporu pre používanie poštových klientov poskytujú správcovia IKT a to len zamestnancom UMB. Technickú podporu je možné poskytnúť pre poštových klientov Microsoft Outlook v posledných dvoch verziách.

## Článok 13
## Zdieľanie pracovných súborov

13.1. V rámci pracovnej činnosti na UMB vznikajú dáta, ku ktorým potrebuje prístup viacero osôb, resp. je potrebný prístup používateľa MS z lokality mimo UMB. Dáta v pracovných súboroch používateľa MS sú uchovávané na pracovných staniciach UMB, na serveroch UMB alebo v cloude Office365.

13.2. Na účel zdieľania bežných pracovných súborov je možné použiť službu OneDrive Office365. Do služby je potrebné sa prihlásiť kontom UMB.

13.3. Ak súbory obsahujú chránené údaje, nesmú opustiť prostredie UMB. Na zdieľanie takýchto súborov je určený IT systém Intranet UMB dostupný na adrese: https://intranet.umb.sk.

13.4. Pre zdieľanie alebo ukladanie akýchkoľvek pracovných súborov sa zakazuje využívanie služieb tretích strán, ktoré nemajú zmluvu s UMB (ako napríklad Dropbox, Google Drive, a pod.)

## Článok 14
## Monitorovanie MS UMB

14.1. Za účelom dodržiavania povinností vyplývajúcich z právnych predpisov SR a EÚ je UMB oprávnená primerane riadiť prevádzku svojej dátovej siete. Prevádzka MS UMB je monitorovaná správcom MS UMB a správcami lokálnych uzlov s cieľom:

a) optimalizovať prevádzku MS UMB;
b) zisťovať chybové stavy a predchádzať im;
c) zabezpečiť ochranu pred neoprávneným prístupom k sieťovým prvkom MS UMB, SANET, Internet;
d) zamedziť porušovaniu platnej legislatívy SR a EÚ.

14.2. Pokiaľ monitorovanie odhalí dôkaz možnej nepovolenej aktivity, bude záznam z monitorovania poskytnutý ako podklad pre prijatie opatrení na okamžité zamedzenie jej pokračovania vrátane prevencie (napríklad okamžité zamedzenie prístupu zariadenia alebo používateľa do MS UMB), disciplinárne konanie v rámci UMB alebo prípadne pre následné trestné konanie. Inak sú tieto

záznamy dôverné a manipulácia s nimi je vykonávaná v súlade s pravidlami pre manipuláciu s dôvernými informáciami v rámci UMB.

14.3. V súvislosti s poskytovaním elektronických komunikačných služieb v sieti UMB zaznamenávajú systémy, ktoré zabezpečujú poskytovanie týchto služieb, prevádzkové a lokalizačné údaje. Bez týchto údajov by nebolo možné služby poskytnúť (sieť by nevedela ako a ktoré zariadenia má prepojiť).

14.4. Prevádzkové a lokalizačné údaje slúžia výlučne na diagnostiku a riešenie problémových stavov (problémy s nefunkčnosťou pripojenia, bezpečnostné incidenty). Tieto údaje nie sú poskytované žiadnej tretej strane, s výnimkou prípadov, v ktorých tak určuje zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov alebo iný právny predpis (napr. na účely poskytovania súčinnosti súdom, orgánom činným v trestnom konaní, iným orgánom štátu) alebo prípadov, kedy sa jedná o používateľa MS z inej akademickej inštitúcie, ktorý využíva službu pripojenia do siete UMB prostredníctvom roamingového systému "eduroam". V takom prípade poskytne poverený technický kontakt na strane UMB súčinnosť s technickým kontaktom na strane domovskej inštitúcie používateľa MS v zmysle a v rozsahu platnej Roamingovej politiky systému "eduroam".

## Článok 15
## Prevádzka webových stránok

15.1. UAKOM poskytuje priestor a technickú podporu pre prevádzku bežných webových stránok pre potreby UMB.

15.2. Webové stránky môžu byť prevádzkované len na doménach, ktoré sú vo vlastníctve UMB. V opačnom prípade je nutný súhlas štatutára UMB.

15.3. Podporované technológie, ktoré môžu webové stránky využívať:
- 15.3.1. Webový server IIS (OS Microsoft Windows);
- 15.3.2. Webový server Apache (OS Linux);
- 15.3.3. ASP (OS Microsoft Windows);
- 15.3.4. PHP (OS Linux);
- 15.3.5. Databázový systém Microsoft SQL Server;
- 15.3.6. Databázový systém MySQL;
- 15.3.7. FTPS prístup v prípade použitia IIS a OS Microsoft Windows;
- 15.3.8. SFTP prístup v prípade použitia OS Linux.

15.4. Ak webová stránka vyžaduje pre svoju prevádzku technológie, ktoré nie sú uvedené v bode 15.3., môže byť žiadosť o webový priestor zamietnutá.

15.5. UAKOM si vyhradzuje právo zamietnuť žiadosť ak hrozí, že webová stránka bude obmedzovať alebo ohrozovať prevádzku iných webových stránok, ktoré UAKOM prevádzkuje napríklad nadmerným zaťažovaním systémov atď.

15.6. Ak je webová stránka vytvorená v niektorom z voľne dostupných redakčných systémov (napríklad WordPress, Drupal, Joomla) musí byť pravidelne aktualizovaná tak, aby obsahovala všetky bezpečnostné záplaty dostupné počas celej doby prevádzky stránky. Ak je verzia redakčného systému vyhlásená jeho tvorcom za nepodporovanú alebo bola jej podpora ukončená z iných dôvodov, je žiadateľ povinný zabezpečiť aktualizáciu stránky na verziu redakčného systému, ktorá má od tvorcu dostupnú podporu.

15.7. Pre vytvorenie webového priestoru a ďalších súvisiacich prác ako je registrácia záznamov v DNS, vytvorenie prístupov do databázových systémov atď. je nutné podať Žiadosť o vytvorenie webového priestoru (príloha 15.7). V žiadosti musí byť definovaná osoba, ktorá bude zodpovedná za realizáciu všetkých technických úkonov týkajúcich sa chodu a údržby webovej stránky, na ktorú sa podávaná žiadosť vzťahuje. Táto osoba bude musieť byť dostupná počas celej doby prevádzky stránky. Ak dôjde k výmene tejto osoby (napríklad kvôli ukončeniu pracovného pomeru alebo

zmene dodávateľa) je žiadateľ povinný o tomto informovať technickú podporu mailom na adresu helpdesk@umb.sk.

15.8. V prípade, že dôjde k bezpečnostnému incidentu alebo bude prevádzka webovej stránky inak ohrozovať akékoľvek IT systémy univerzity, je správca webového servera oprávnený prevádzku webovej stránky okamžite ukončiť alebo obmedziť tak, aby nedochádzalo k ohrozovaniu týchto IT systémov. Žiadateľ, respektíve zodpovedná osoba, je povinná na výzvu správcu webového servera bezodkladne zabezpečiť nápravu a informovať správcu webového servera o vykonaných úkonoch.

## Článok 16
## Postup pri nahlasovaní porúch a problémov

16.1. Ak má zamestnanec problémy pri práci s IT systémom UMB, kontaktuje správcu IKT organizačnej jednotky, na ktorej pracuje. Správcu IKT kontaktuje aj v prípade, že uvedený problém nastal v súvislosti s niektorým z centrálnych IT systémov. Alternatívne môže kontaktovať technickú podporu mailom na adrese helpdesk@umb.sk .

16.2. Ak má študent problémy pri práci s IT systémom UMB, kontaktuje technickú podporu mailom na adresu helpdesk@umb.sk .

16.3. Pri kontaktovaní technickej podpory mailom musí správa obsahovať:
   a) meno a priezvisko používateľa MS;
   b) organizačnú jednotku, na ktorej pracuje alebo názov študijného programu, ktorý študuje;
   c) podrobný opis problému.

16.4. Návody na konfiguráciu zariadení a používanie IT systémov sa nachádzajú na stránke https://helpdesk.umb.sk.

16.5. V prípade problémov s mailovým systémom je pre zamestnancov k dispozícii možnosť kontaktovať technickú podporu UAKOM aj mimo pracovných hodín na telefónnom čísle 0917 863 568 a to od 7:00 do 21:00 hod. v pracovných dňoch a od 9:00 do 16:00 v deň pracovného voľna, cez sviatok alebo počas celouniverzitných dovoleniek. Táto podpora nie je k dispozícii pre študentov a netýka sa iných systémov ako mailového.

# TRETIA ČASŤ
# ZÁVEREČNÉ USTANOVENIA

17.1. Neoddeliteľnou súčasťou tejto smernice sú jej prílohy: Príloha č. 04.6 Žiadosť o vytvorenie osobitného prístupu do WiFi, Príloha č. 06.2a Plán zálohovania IS na UMB, Príloha č. 06.2b Protokol z testu obnovy záloh, Príloha č. 08.1 Žiadosť o výmaz dát zo servera a príslušnej infraštruktúry, Príloha č. 10.2 Žiadosť o vzdialený prístup do pracovnej stanice používateľa MS, Príloha č. 10.3 Žiadosť o sprístupnenie dát používateľa MS, Príloha č. 12.8 Žiadosť o zmenu mailovej adresy, Príloha č. 12.9 Žiadosť o vytvorenie osobitnej e-mailovej adresy, Príloha č. 12.14a Žiadosť o nahliadnutie do mailovej schránky, Príloha 12.14b Protokol o nahliadnutí do mailovej schránky, Príloha č. 15.1 Žiadosť o vytvorenie webového priestoru.

17.2. Táto Smernica má celouniverzitnú platnosť. Za dodržiavanie tejto smernice sú zodpovední všetci zamestnanci UMB, doktorandi a študenti UMB a ďalší používatelia MS UMB definovaní v bode 2.17 tejto smernice.

17.3. Každý používateľ MS je povinný oboznámiť sa s pravidlami používania MS a s touto smernicou.

17.4. Zamestnávateľ je povinný zamestnancov o tejto smernici preukázateľne informovať. Informovanie zabezpečuje UAKOM. Záznamy o oboznámení zamestnancov s touto smernicou (menné zoznamy s podpismi zamestnancov) sú uložené na pracovisku UAKOM a na požiadanie je UAKOM povinný predložiť ich v prípade kontroly (napr. kontroly z oblasti ochrany osobných údajov, NKÚ a pod.)

17.5. Nadobudnutím účinnosti tejto smernice sa ruší Smernica č. 6/2004 Prevádzkový poriadok Metropolitnej siete UMB. Ruší sa Smernica č. 14/2004 o povinných štruktúrach www stránok pracovísk UMB a zásadách zverejňovania informácií na www stránkach UMB, ako aj Dodatok č. 1/2005 ku smernici 14/2004. Ruší sa Smernica č. 10/2010 Pravidlá používania a správy e-mailovej komunikácie zamestnancov Univerzity Mateja Bela v Banskej Bystrici.

17.6. Táto smernica, predovšetkým článok 12, bod 12.14., ako aj článok 14, boli prerokované so zástupcami zamestnancov dňa 2. 5. 2018.

17.7. Táto smernica nadobúda platnosť dňom podpisu rektorom UMB a účinnosť dňom 25. 05. 2018.

doc. Ing. Vladimír Hiadlovský, PhD.
rektor UMB

Mgr. Zuzana Piliarová
predseda Rady ZO OZ

Príloha č. 1

Ak zamestnávateľ potrebuje z určitých dôvodov zaviesť kontrolný mechanizmus (monitorovať činnosť svojich zamestnancov), musí o tom zamestnancov **najskôr informovať.** Nepotrebuje k tomu ich súhlas, právnym základom pre spracúvanie osobných údajov je totiž Zákonník práce a jeho § 13 ods. 4, podľa ktorého:

*„Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručenú na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania".*

## INFORMOVANIE ZAMESTNANCA

## O ZAVEDENÍ KONTROLNÉHO MECHANIZMU

Názov prevádzkovateľa: .....

Sídlo: .....

Identifikačné číslo: .....

Prevádzkovateľ týmto informuje zamestnanca .....,

*(titul, meno, priezvisko zamestnanca),*

že:

- pracovné e-mailové schránky

- činnosť zamestnanca v metropolitnej sieti UMB

podliehajú kontrolnému mechanizmu v zmysle § 13 ods. 4 zákona č. 311/2001 Z. z. Zákonníka práce.

Kontrolný mechanizmus vykonáva prevádzkovateľ **na účely a spôsobom** uvedeným v Smernici o Prevádzkovom poriadku Metropolitnej siete UMB č. ? /2018 zo dňa ... , č. sp. ....., č. z..... (ďalej len „Smernica") v Čl. 12 bode 14 a v Čl. 14., prípadne za účelom vyvodenia pracovnoprávnej zodpovednosti voči príslušnému zamestnancovi. Kontrolný mechanizmus vykonáva prevádzkovateľ u zamestnanca **po dobu** trvania jeho pracovno-právneho vzťahu.

Svojim podpisom zamestnanec potvrdzuje, že bol o kontrolnom mechanizme informovaný a že sa oboznámil so Smernicou.

V ..... dňa: .....

.....

podpis zamestnanca

Príloha č. 04.6

**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Žiadosť o vytvorenie osobitného prístupu do WiFi sietí

*(túto žiadosť je možné podať elektronicky zaslaním jej naskenovanej kópie na adresu helpdesk@umb.sk)*

| | |
|---|---|
| **Názov podujatia:** | *Konferencia UNINFOS 2016* |
| **Cieľová skupina:** | *Účastníci z prostredia slovenských a zahraničných vysokých škôl.* |
| **Miesto a čas konania:** | *Aula Rotunda, EF UMB* |
| **Predpokladaný počet účastníkov:** | *150* |
| **Kontaktná osoba:** | *Jozef Siláči, jozef.silaci@umb.sk, +421 908 540 717* |

**Žiadateľ**

Meno: Dátum: Podpis:

Príloha č. 06.2a

Univerzita Mateja Bela

Národná 12, 974 01 Banská Bystrica

# Plán zálohovania IS na UMB

| Názov IS: | jedalen.umb.sk | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| **Zálohovanie serverov, na ktorých je IS prevádzkovaný:** | | | | | | |
| **Názov servera** | **IP** | **Zálohovanie diskov alebo adresárov** | **Záloha na úrovni aplikácie** | **Záloha stavu systému[1]** | **Frekvencia zálohovania** | **Retencia zálohovania[2]** |
| *jedalen.umb.sk* | *194.160.44.5* | *c:\users d:\data* | *SQL Server* | *áno* | *24 hodín* | *10 dní* |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Vypracoval**

Meno: Dátum: Podpis:

**Prevzal**

Meno: Dátum: Podpis:

1. **Záloha stavu systému** - záloha nastavení operačného systému.
2. **Retencia zálohovania** - doba po ktorú sa uchovávajú zálohy.

**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Test obnovy IS na UMB

| **Názov IS:** | *jedalen.umb.sk* | | | | |
|---|---|---|---|---|---|
| **A – systém v správe UMB** | | | | | |
| **Priebeh testu obnovy jednotlivých súčastí IS:** | | | | | |
| **Dátum** | **Názov servera** | **IP** | **Obnova obsahu adresárov** | **Obnova na úrovni IS** | **Obnova system state** |
| *1.1.2018* | *jedalen.umb.sk* | *194.160.44.5* | *obnova bola úspešná* | | |
| *2.1.2018* | *jedalen.umb.sk* | *194.160.44.5* | | *obnova bola úspešná* | *obnova bola úspešná* |
| | | | | | |
| | | | | | |
| **Výsledok testu** | | | | | |
| Bol systém po teste obnovy plne funkčný? | | | *Áno* | *Nie* | *Netestované* |
| Časová náročnosť úplnej obnovy systému (v hodinách): | | | *48* | | |
| **Poznámky:** (V prípade, že nebola funkčnosť obnoveného systému testovaná, sem napísať odôvodnenie.) | | | | | |
| **Dôvody zlyhania:** (Vyplňuje sa len v prípade, že obnova nebola úspešná.) | | | | | |
| **Prijaté opatrenia:** (Vyplňuje sa len v prípade, že obnova nebola úspešná.) | | | | | |
| **B – systém spravovaný externým dodávateľom** | | | | | |
| **Názov spoločnosti:** | | | | | |
| **Zmluvný vzťah:** *Uveďte áno alebo nie* | | | | | |
| **Kontaktná osoba:** Meno a priezvisko: | | Telefón: | | e-mail: | |
| **V prípade, že je systém spravovaný externým dodávateľom je neoddeliteľnou súčasťou protokolu potvrdenie od dodávateľa, že zálohované dáta postačujú na úplnú obnovu systému (vytlačený mail alebo iný dokument).** | | | | | |

**Vypracoval**

Meno: Dátum: Podpis:

**Prevzal**

Meno: Dátum: Podpis:

Príloha č. 08.1

**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Žiadosť o výmaz dát zo servera a príslušnej infraštruktúry

| | |
|---|---|
| **Osoba zodpovedná za dáta:** | *Martin Miklík* |
| **Informačný systém/server:** | *Intranetový portál UMB (intranet.umb.sk)* |
| **Obsahuje systém chránené údaje?** | *Áno* |
| **Poznámky:** | *Dáta nebudú potrebné po 31. 8. 2018* |

**Žiadateľ**

Meno: Dátum: Podpis:

**Prevzal**

Meno: Dátum: Podpis:

Príloha č. 10.2


**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Žiadosť o vzdialený prístup do pracovnej stanice používateľa

| | |
|---|---|
| **Žiadateľ:** | *Martin Miklík* |
| **Dôvod / účel žiadosti:** | *Potrebný prístup na PC aj mimo kancelárie alebo počas pracovných ciest.* |
| **IP adresa pracovnej stanice:** | *194.160.39.256* |
| **Názov pracovnej stanice:** | *R-PC-0012* |

**Žiadateľ**

Meno: Dátum: Podpis:

**Prevzal**

Meno: Dátum: Podpis:

Príloha č. 10.3

**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Žiadosť o sprístupnenie dát používateľa MS

| | |
|---|---|
| **Žiadateľ:** | *Martin Miklík* |
| **Žiadam sprístupniť pracovné dáta používateľa:** | *Miroslav Oráč* |
| **Dôvod sprístupnenia dát:** | *Používateľ je na dlhodobej PN a v jeho počítači sa nachádzajú údaje potrebné pre vyriešenie bezpečnostného incidentu.* |
| **Umiestnenie dát:** | *Uveďte ak viete, kde dáta sa nachádzajú (pracovná stanica, cloudové úložisko, ...)* |
| **Žiadam sprístupniť tieto dáta:** | *Informácie o IP adresách pracovných staníc.* |

**Žiadateľ**

Meno: Dátum: Podpis:

**Prevzal**

Meno: Dátum: Podpis:

Príloha č. 12.8


**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Žiadosť o zmenu e-mailovej adresy

*(túto žiadosť je možné podať elektronicky zaslaním jej naskenovanej kópie na adresu helpdesk@umb.sk)*

| | |
|---|---|
| **Žiadateľ:** | *Gilbert Elliot-Murray-Kynynmound* |
| **Pôvodná e-mailová adresa:** | *Gilbert.Elliot-Murray-Kynynmound@umb.sk* |
| **Požadovaná e-mailová adresa:** | *Gilbert.Murray@umb.sk* |
| **Dôvod zmeny e-mailovej adresy:** | *Pôvodná mailová adresa je príliš dlhá.* |

**Žiadateľ**

Meno: Dátum: Podpis:

Príloha č. 12.9

**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Žiadosť o vytvorenie osobitnej e-mailovej adresy

*(túto žiadosť je možné podať elektronicky zaslaním jej naskenovanej kópie na adresu helpdesk@umb.sk)*

| | |
|---|---|
| **Žiadateľ (meno a priezvisko, pracovisko, e-mail, tel.):** | *Miroslav Oráč, UAKOM, miroslav.orac@umb.sk, 048 /446 6812* |
| **Účel vytvorenia e-mailovej adresy:** | *Vytvorenie distribučného zoznamu pre správcov IKT.* |
| **Navrhovaný tvar e-mailovej adresy:** | *sprava.ikt@umb.sk* |
| **Doba platnosti e-mailovej adresy:** | **Od:** *23.2.2018* |
| | **Do:** *na neurčito* |
| **Žiadateľ požaduje možnosť odosielania z navrhovaného e-mailu:** | *nie* |
| **Zoznam osôb v prípade distribučného zoznamu:** | *janko.mrkvicka@umb.sk, michal.modry@umb.sk, ...* |
| Ak je potrebná zmena súvisiaca s e-mailovou adresou, informujte správcu e-mailom na adresu: helpdesk@umb.sk | |

**Žiadateľ**

Meno: Dátum: Podpis:

Príloha č. 12.14a

**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Žiadosť o nahliadnutie do e-mailovej schránky zamestnanca

| | | |
|---|---|---|
| **Žiadateľ:** | *Martin Miklík* | |
| **Žiadam o sprístupnenie e-mailovej schránky zamestnanca:** | **Meno** | *Miroslav Oráč* |
| | **Osobné číslo** | *8745* |
| | **Mailová schránka** | *miroslav.orac@umb.sk* |
| **Dôvod sprístupnenia e-mailovej schránky:** | *Zamestnanec je hospitalizovaný a do jeho mailovej schránky boli doručené dokumenty, ktoré sú nevyhnutné pre uzatvorenie verejného obstarávania na predmet zákazky ... (cenová ponuka od súťažiaceho ...).*<br>*Je ohrozené dodržanie zákonných termínov.* | |
| **Spôsob a výsledok pokusu o kontaktovanie zamestnanca** | *Tu sa uvádzajú sa všetky spôsoby, ktorými sa žiadateľ pokúsil kontaktovať zamestnanca. Vždy uvádzajte aj čas a výsledok pokusu o kontakt.*<br>*Príklady:*<br>1. *telefonát na služobný mobil, 22.2.2018 10:00, nedovolal som sa*<br>2. *telefonát na služobný mobil, 22.2.2018 10:00, zamestnanec súhlasil s nahliadnutím, pretože nemá prístup k PC.* | |

**Žiadateľ**

Meno: Dátum: Podpis:

**Vyjadrenie osoby zodpovednej za ochranu osobných údajov**

Meno: Dátum: Podpis:

Súhlasím / Nesúhlasím[1] s nahliadnutím do mailovej schránky zamestnanca.

**Vyjadrenie IT bezpečnostného správcu UAKOM**

Meno: Dátum: Podpis:

Súhlasím / Nesúhlasím[1] s nahliadnutím do mailovej schránky zamestnanca.

**Prevzal**

Meno: Dátum: Podpis:

1. Nehodiace sa preškrtnite

Príloha č. 12.14b

**Univerzita Mateja Bela**

**Národná 12, 974 01 Banská Bystrica**

# Protokol o nahliadnutí do e-mailovej schránky

| | |
|---|---|
| **Prítomné osoby (vrátane správcu mailového systému)** | |
| **Názov mailovej schránky** | |
| **Čas a dátum prístupu do schránky** | |
| **Údaje o sprístupnených správach (odosielateľ, predmet správy, čas a dátum doručenia)** | |
| **Spôsob odovzdania sprístupnených správ žiadateľovi** | *Príklady: správy boli vytlačené, správy boli uložené na USB kľúč žiadateľa, žiadateľ si správy len prečítal a neboli nikam kopírované, atď.* |

| | **Meno** | **Podpis** |
|---|---|---|
| **Správca mailového systému, ktorý vykonal sprístupnenie údajov** | | |
| **Žiadateľ** | | |
| **Ďalšie prítomné osoby** | | |
| | | |
| | | |
| | | |