STU

Metodické usmernenie na vykonanie ustanovení Prevádzkovej bezpečnostnej smernice informačného systému STU

Centrum výpočtovej techniky STU

09.06.2025

Obsah

1. Úvod

Informačný systém je kľúčovým nástrojom pre efektívne fungovanie každej inštitúcie, vrátane Slovenskej technickej univerzity v Bratislave (ďalej len „STU“ alebo „univerzita“). Tento systém zahŕňa hardvér, softvér, dáta, elektronickú komunikáciu a pod. Neoddeliteľnou súčasťou jeho správnej prevádzky sú nielen zamestnanci, ktorí ho spravujú, ale aj používatelia, ktorí ho využívajú pri plnení svojich pracovných úloh. Efektívne a zodpovedné používanie informačného systému na STU prispieva k úspešnému fungovaniu univerzity a zvyšuje kvalitu a produktivitu práce jej zamestnancov.

STU ako prevádzkovateľ spracúvania osobných údajov, má povinnosť dodržiavať predpisy vyplývajúce z článku 32 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane osobných údajov (ďalej len „GDPR“) a zo zákona č. 18/2018 Z.z. o ochrane osobných údajov (ďalej len „Zákon o OOÚ“). V rámci týchto povinností musí univerzita implementovať potrebné technické a organizačno-právne opatrenia na zaistenie bezpečnosti a ochrany prístupu v rámci svojej technickej infraštruktúry. Tieto opatrenia zahŕňajú používanie aktuálnych verzií operačných systémov, databázových a sieťových programov, antivírusovej ochrany a bezpečnostných prvkov na ochranu počítačovej siete STU a zariadení zapojených do tejto siete, ako aj mimo nej.

Toto Metodické usmernenie na vykonanie ustanovení Prevádzkovej bezpečnostnej smernice informačného systému STU (ďalej len „Metodické usmernenie“) k Smernici rektora číslo: 1/2019 – SR Prevádzková bezpečnostná smernica informačného systému Slovenskej technickej univerzity v Bratislave (ďalej len „Smernica“) stanovuje rámec pre bezpečnú a spoľahlivú prevádzku informačného systému STU. Je navrhnuté tak, aby jeho dodržiavanie zamestnancami a študentmi univerzity chránilo pred neoprávneným prístupom do dátovej siete STU, a ochránilo tak integritu informačných systémov STU. Metodické usmernenie tiež určuje postupy na ochranu pred počítačovými vírusmi a na prevenciu možnej straty alebo zmeny dát, vrátane ochrany osobných údajov zamestnancov a študentov.

Tento dokument zároveň definuje pravidlá používania informačného systému, Internetu, Intranetu a elektronickej pošty zo strany používateľov na STU.

Vzhľadom na to, že všetky IT prostriedky vrátane dát a aplikácií sú majetkom STU, je toto metodické usmernenie zamerané na ochranu univerzity pred ich možným zneužitím, poškodením alebo odcudzením zo strany používateľov, ako aj pred neoprávneným prístupom, útokmi a inými vonkajšími hrozbami.

1.1 Definícia pojmov

Aktívum – akýkoľvek prvok informačného systému, ktorý má hodnotu pre organizáciu a je nevyhnutný pre jej činnosť. Môže zahŕňať hardvér, softvér, dáta, informačné systémy, sieťovú infraštruktúru, dokumenty, ľudské zdroje a iné zdroje, ktoré sú potrebné na zabezpečenie služieb, procesov a funkcií organizácie.

Analýza rizík – proces preskúmania vzťahov medzi aktívami, hrozbami, bezpečnostnými slabinami a opatreniami, ktorý zahŕňa hodnotenie pravdepodobnosti a dopadu rizík s cieľom určiť aktuálnu úroveň bezpečnostných rizík a navrhnúť opatrenia na ich zmiernenie alebo elimináciu.

Autentifikácia (identifikácia) – bezpečnostný mechanizmus na overenie identity používateľa, ktorý chce získať prístup k chráneným aktívam.

Autorizácia (overenie oprávnenia) – bezpečnostný mechanizmus na určenie úrovne prístupu alebo oprávnení udelených autentifikovanému používateľovi na základe jeho identity, funkcie alebo privilégií na interakciu s konkrétnymi aktívami.

Bezpečnostná brána (Firewall) – bezpečnostné zariadenie alebo softvérový nástroj, ktorý slúži na kontrolu a filtrovanie sieťovej komunikácie medzi rôznymi časťami informačného systému alebo medzi vnútornou sieťou a externými sieťami, ako je Internet. Firewall umožňuje alebo blokuje prenos dát na základe vopred definovaných bezpečnostných pravidiel, čím chráni systém pred neoprávneným prístupom, kybernetickými útokmi a ďalšími bezpečnostnými hrozbami.

Bezpečnostná hrozba – potenciálna udalosť, činnosť, entita alebo okolnosť, ktorá môže využiť bezpečnostnú slabinu v informačnom systéme a spôsobiť narušenie dôvernosti, integrity alebo dostupnosti údajov a služieb. Bezpečnostné hrozby môžu byť úmyselné (napr. kybernetické útoky, malware, phishing) alebo neúmyselné (napr. ľudské chyby, zlyhanie hardvéru, prírodné katastrofy).

Bezpečnostná slabina (zraniteľnosť) – chyba, nedostatok alebo slabé miesto v informačnom systéme, softvéri, hardvéri, sieťovej infraštruktúre alebo bezpečnostných postupoch, ktoré môže byť zneužité na narušenie dôvernosti, integrity alebo dostupnosti systému alebo údajov. Bezpečnostná slabina môže vzniknúť v dôsledku chybného návrhu, nesprávnej konfigurácie, chýbajúcej aktualizácie, alebo chýbajúceho, nedostatočného alebo nesprávne implementovaného bezpečnostného opatrenia.

Bezpečnostné opatrenie – akcia, mechanizmus, proces, technológia alebo postup implementovaný s cieľom chrániť informačné systémy, údaje a služby pred bezpečnostnými hrozbami a zraniteľnosťami. Príklady bezpečnostných opatrení zahŕňajú šifrovanie dát, firewally, antivírusový softvér, autentifikačné systémy, bezpečnostné školenia pre zamestnancov, pravidelné zálohovanie dát, pravidelné aktualizácie softvéru a fyzickú ochranu zariadení.

Bezpečnostné riziko – pravdepodobnosť a potenciálny dopad hrozby, ktorá môže narušiť bezpečnosť informačného systému. Riziko sa vyjadruje ako miera možnej škody spôsobenej hrozbou využívajúcou slabinu v systéme, pričom závisí od pravdepodobnosti zneužitia zraniteľnosti a závažnosti vzniknutej škody (dôsledku).

Bezpečnostný incident – udalosť alebo séria udalostí, ktoré vedú k porušeniu bezpečnostných politík, štandardov alebo postupov, pričom majú negatívny vplyv na dôvernosť, integritu alebo dostupnosť informačných systémov, údajov alebo služieb. Bezpečnostný incident môže zahŕňať neoprávnený prístup k systémom, narušenie dát, útoky typu malware, phishing, výpadky služieb, krádež údajov alebo akékoľvek iné aktivity, ktoré ohrozujú bezpečnosť organizácie.

Bezpečnostný manažér IT (CISO) – odborník zodpovedný za plánovanie, implementáciu, správu a presadzovanie bezpečnostnej politiky, stratégií a opatrení na ochranu informačných systémov a technológií.

BYOD (Bring Your Own Device) – politika, ktorá umožňuje zamestnancom alebo iným autorizovaným používateľom používať svoje vlastné osobné zariadenia, ako sú smartfóny, tablety alebo notebooky, na prístup k informačným systémom, aplikáciám a dátam v sieti STUNET.

Centrum výpočtovej techniky STU (CVT STU) – Centrálne IT pracovisko STU.

DMZ (Demilitarizovaná zóna) – bezpečnostná zóna v počítačovej sieti, ktorá slúži ako izolovaný segment medzi internou sieťou organizácie a externými sieťami, ako je Internet. DMZ obsahuje servery a iné verejne prístupné zariadenia (napríklad webové servery, e-mailové servery), ktoré musia byť prístupné z Internetu, ale sú oddelené od citlivejších častí internej siete. Toto usporiadanie poskytuje dodatočnú vrstvu ochrany, pretože ak dôjde k napadnutiu zariadení v DMZ, vnútorná sieť zostáva chránená.

Dostupnosť – vlastnosť IS, ktorá zaisťuje, že autorizovaní používatelia majú nepretržitý a spoľahlivý prístup k potrebným informáciám, údajom a zdrojom vtedy, keď ich potrebujú. Dostupnosť zahŕňa ochranu systémov a služieb pred výpadkami, útokmi a inými udalosťami, ktoré by mohli znemožniť alebo obmedziť prístup k týmto zdrojom.

Dôsledok – výsledok alebo následok bezpečnostného incidentu, ohrozenia alebo narušenia, ktorý ovplyvňuje integritu, dôvernosť alebo dostupnosť informačného systému, jeho údajov a služieb. Dôsledky môžu zahŕňať finančné straty, právne následky, poškodenie reputácie, stratu dát, prerušenie prevádzky alebo iné negatívne vplyvy na univerzitu alebo jej používateľov.

Dôvernosť – vlastnosť IS, ktorá zabezpečuje, že informácie a údaje sú prístupné iba oprávneným osobám alebo systémom, a sú chránené pred neautorizovaným prístupom alebo zverejnením. Pod prístupom sa rozumie zobrazenie, skopírovanie, vytlačenie údajov, i samotné zistenie faktu, že došlo k prenosu (uloženiu) údajov.

Eduroam – celosvetová prístupová služba, ktorá umožňuje študentom, výskumným pracovníkom a zamestnancom zúčastnených inštitúcií získať pripojenie na Internet v rámci univerzitného areálu a v priestoroch zúčastnených inštitúcií pomocou prístupových údajov z domácej inštitúcie.

Informačné technológie (IT) – súbor technológií a infraštruktúry používaných na spracovanie informácií. IT zahŕňa technológie potrebné na prevádzku a údržbu informačných systémov, dátových sietí a aplikácií.

Informačný systém (IS) – integrovaný súbor komponentov – zahŕňajúci hardvér, softvér, dáta a procedúry – ktoré sú navrhnuté na zber, ukladanie, spracovanie a distribúciu informácií. Tieto systémy môžu byť použité na správu, analýzu a organizáciu údajov, vrátane osobných údajov, a slúžia na podporu činností a rozhodovacích procesov univerzity. Informačný systém zahŕňa všetky procesy a technológie potrebné na efektívne spracovanie a ochranu osobných údajov, vrátane zabezpečenia ich dôvernosti, integrity a dostupnosti.

Integrita – vlastnosť IS, ktorá zabezpečuje ochranu údajov pred neautorizovanou modifikáciou, neúmyselnými chybami a poškodením, a ktorá zaručuje, že údaje zostávajú verné svojmu pôvodnému stavu počas ich spracovania, ukladania a prenosu.

Interval zálohovania (časová frekvencia zálohovania) – interval medzi časmi vytvárania dvoch po sebe nasledujúcich záloh dát. Kratší interval zálohovania znižuje riziko straty dát, ale môže vyžadovať viac úložného priestoru a zdrojov na spracovanie záloh.

Metodik aplikácie – zamestnanec CVT STU, ktorý špecifikuje funkčné požiadavky aplikácie alebo modulu IS, zúčastňuje sa akceptačného testovania a školenia používateľov.

MFA (Multifactor Authentication) – viacfaktorová autentifikácia – bezpečnostný proces, ktorý vyžaduje overenie identity používateľa pomocou dvoch alebo viacerých nezávislých faktorov, napríklad kombinácie hesla a bezpečnostného zariadenia, certifikátu, push notifikácie alebo jednorazového TOTP kódu v mobilnej aplikácii.

Podporná technická infraštruktúra – technické zariadenia, ktoré plnia podporné funkcie zabezpečujúce požadované prevádzkové podmienky IT (napr. záložné napájacie zdroje, klimatizácia a pod.).

Používateľ – autorizovaná osoba, ktorá používa informačné technológie a systémy na vykonávanie svojich študijných, pracovných alebo osobných úloh ako koncový používateľ.

Požiadavka – formalizovaná žiadosť používateľa o IT službu, úpravu nastavenia, technickú podporu alebo informáciu, spracúvaná podľa štandardizovaných postupov IT útvaru. Najčastejšie sa eviduje ako tiket v aplikácii Helpdesk, prípadne môže byť podaná

e-mailom, papierovým formulárom alebo správou, vždy podľa interných pravidiel a stanovených procesov príslušného IT útvaru.

Programové vybavenie (softvér) – súbor programov, aplikácií a systémových nástrojov, ktoré riadia a koordinujú činnosť hardvéru, umožňujú prácu s údajmi a poskytujú rôzne služby a funkcie informačného systému, vrátane operačných systémov, firmvéru, databázového softvéru, bezpečnostných aplikácií a používateľských programov.

Riadenie prístupu – proces a súbor postupov na kontrolu, kto má oprávnenie pristupovať k jednotlivým aktívam informačného systému, a to na základe stanovených pravidiel a politiky organizácie. Cieľom riadenia prístupu je zabezpečiť, aby iba autorizovaní používatelia mali prístup k citlivým informáciám, systémom a zdrojom, čím sa minimalizuje riziko neoprávneného prístupu, zneužitia alebo úniku dát. To zahŕňa autentifikáciu, autorizáciu, prideľovanie a revíziu prístupových práv.

RPO (Recovery Point Objective) - maximálna prípustná strata dát, ktorá môže nastať v prípade incidentu alebo výpadku systému. RPO určuje, ako staré môžu byť dáta, ktoré sa použijú na obnovu, alebo aký časový interval je prijateľný medzi poslednou zálohou a časom incidentu.

RTO (Recovery Time Objective) – maximálny čas, ktorý je prípustný na obnovu systému alebo dát po výpadku alebo incidente, aby sa minimalizoval dopad na prevádzku. RTO stanovuje, ako rýchlo musí byť systém alebo dáta obnovené, aby sa splnili požiadavky na prevádzkovú kontinuitu a minimalizovali sa škody spôsobené výpadkom.

SANET (Slovenská akademická dátová sieť) – vysokorýchlostná sieť pre vedu, výskum a vzdelávanie, ktorú prevádzkuje nezisková organizácia Združenie používateľov Slovenskej akademickej dátovej siete SANET.

STUNET – dátová sieť STU. Pre účely tohto Metodického usmernenia sa pojmom STUNET myslí celá IT infraštruktúra STU (všetky technické prostriedky a programové vybavenie, vrátane sieťovej, serverovej, desktopovej a podpornej technickej infraštruktúry).

Šifrovanie – proces konverzie čitateľných údajov (plaintext) do nečitateľnej formy (ciphertext) pomocou kryptografického algoritmu a šifrovacieho kľúča, aby boli chránené pred neoprávneným prístupom. Šifrovanie zabezpečuje, že len oprávnené strany, ktoré majú správny dešifrovací kľúč, môžu údaje prečítať a pochopiť ich obsah. Používa sa na ochranu citlivých informácií pri prenose po sieti, ako aj pri ich ukladaní, čím zvyšuje dôvernosť a integritu údajov.

Technické prostriedky (hardvér) – fyzické komponenty informačného systému, vrátane zariadení, ako sú servery, počítače, sieťové zariadenia, úložiská, periférie a iné elektronické vybavenie, ktoré zabezpečujú funkčnosť systému a umožňujú spracovanie, ukladanie a prenos dát.

Útvar pre informačné technológie (IT útvar) – organizačný útvar súčasti STU, ktorý zodpovedá za oblasť IT, a plní povinnosti uvedené v Smernici a v tomto Metodickom usmernení.

Vlastník aktíva – organizačný útvar, ktorý zodpovedá za funkčnosť, ochranu, správu a riadenie prístupu ku konkrétnemu aktívu. Vlastník aktíva má zodpovednosť za určenie požiadaviek na ochranu, zabezpečenie primeraných bezpečnostných opatrení, a monitorovanie ich účinnosti, aby sa zabezpečila bezpečnosť a dostupnosť aktíva. V podmienkach STU je vlastníkom aktíva ten organizačný útvar, ktorý v zmysle pracovných povinností zhromažďuje, spracúva a archivuje príslušné dáta (údaje, informácie), napr. vlastníkmi dát o štúdiu a študentoch sú študijné oddelenia súčastí STU.

Zodpovedná osoba – je osoba zodpovedná za implementáciu celkovej bezpečnostnej politiky, jej presadzovanie a udržiavanie, je ustanovená v zmysle §44 Zákona o OOÚ. Za výkon funkcie zodpovedá rektorovi STU (vedúcemu zamestnancovi súčasti STU).

2. Vymedzenie činnosti zamestnancov a študentov STU

V tejto časti sú špecifikované činnosti súvisiace s bezpečnou a spoľahlivou prevádzkou a používaním informačného systému pre jednotlivé skupiny zamestnancov a študentov.

2.1 Systémový administrátor IT

1. Inštaluje systémové programy (predovšetkým operačné systémy).
2. Manipuluje s diskovými médiami a tlačiarňami.
3. Je zodpovedný za plnú prevádzkyschopnosť systémových prostriedkov a nástrojov.
4. Zriaďuje nové používateľské kontá, prideľuje pre ne základné prístupové práva a preveruje oprávnenosť prístupových práv a používateľských kont. Rovnako ruší používateľské kontá.
5. Zodpovedá za zálohovanie a archiváciu systémových a používateľských dát, za archív a vedenie evidencie záložných médií a ich bezpečné uloženie. Rieši havarijné stavy.
6. Denne náhodne monitoruje činnosť používateľov. Činnosti používateľov sa zaznamenávajú do auditných záznamov (logovacie súbory), ktoré sa vyhodnocujú a archivujú.
7. Pravidelne kontroluje stav technických súčastí informačného systému.
8. Raz týždenné nastavuje a kontroluje stav serverov.

2.2 Správca siete IT

1. Podľa požiadaviek bezpečnostnej politiky nastavuje prístupové práva na aktívnych sieťových prvkoch a komunikačných zariadeniach.
2. Pravidelne monitoruje stav siete pomocou programových nástrojov pre riadenie siete.

3. Udržuje v aktuálnom stave informácie o topológii siete, aktívnych a pasívnych prvkoch, o ich parametroch a nastaveniach. Rieši havarijné stavy.
4. Podrobný popis práv a povinností správcov chrbticovej siete a lokálnych sietí súčastí STU je uvedený v kapitole 5.4.

2.3 Databázový administrátor IT (privilegovaný používateľ)

1. Zriaďuje a eviduje a ruší kontá používateľov a skupín, pravidelne preveruje oprávnenosť používateľských kont a prípadne prístupových práv.
2. Vykonáva pravidelný audit databáz a pravidelne ich vyhodnocuje a zálohuje.
3. Uskutočňuje pravidelnú údržbu databáz, monitorovanie ich priestorových nárokov, optimálne nastavovanie parametrov databáz v závislosti od stavu operačného systému a od aktuálnej situácie v databázach.
4. Rieši havarijné stavy podľa havarijného poriadku, pri haváriách obnovuje dáta, funkčnosť databáz a konzultuje neštandardné stavy s dodávateľskými firmami.
5. Testuje a nasadzuje nové databázové softvéry, prípadne ich update a upgrade.
6. Zálohuje databázy a kontroluje pravidelnosť a spoľahlivosť prevádzky z hľadiska obnovy databáz po poškodení dát a obnovy databáz k dátumu.
7. Archivuje systémové a používateľské dáta databáz a vedie evidenciu záložných médií a archívu.
8. Denne námatkovo monitoruje činnosť používateľov. Činnosti používateľov sa zaznamenávajú do auditných záznamov (logovacie súbory), ktoré sa vyhodnocujú a archivujú.
9. Kontroluje v logovacích súboroch oprávnenosť vstupu do databázy (ochrana pred neoprávneným vstupom), zisťuje či bola prekonaná bezpečnostná brána a ak bola, tak preveruje postup jej prekonania.
10. Spolupracuje s ostatnými oddeleniami pri testovaní, výberovom konaní pre nový softvér.
11. Tvorí a spolupodieľa sa na tvorbe návrhov smerníc, upresnení a školení súvisiacich s bezpečnosťou informačných systémov.

2.4 Technik IT

1. Odstraňuje technické poruchy a závady na zariadeniach IT a to buď svojpomocne, napr. výmenou súčiastky, časti dielu alebo celého dielu za nový v rámci záručných podmienok, alebo formou doručenia chybného zariadenia do príslušného servisného strediska alebo dohovoru o oprave cez dodávateľa daného zariadenia.
2. Realizuje technické prepojenia lokálnych počítačových sietí na súčastiach a pracoviskách STU.
3. Pripája zariadenia IT do elektrickej siete napájania a do počítačovej siete STU - STUNET.
4. Prepája jednotlivé zariadenia IT medzi sebou.

5. Na základe príkazov priameho nadriadeného a bezpečnostného manažéra IT vykonáva fyzickú kontrolu nainštalovaného softvéru na PC a o výsledku im podá písomnú správu.
6. Vykonáva previerku zariadení IT, ktoré podliehajú pravidelnému technickému auditu s tým, že pripravuje inováciu zariadení IT, tak, aby na nich bolo možné inštalovať najnovšie verzie operačných, systémových a aplikačných programových produktov.
7. Dôsledne aplikuje opravy (patche) odporúčané výrobcom pre operačné systémy a systémové programy na všetkých inštalovaných zariadeniach IT na STU v okruhu svojej pôsobnosti.

2.5 Používateľ IT

1. Používa PC, operačný systém na ňom nainštalovaný, ako aj všetky aplikácie, na ktoré dostal oprávnenie.
2. Prihlasuje sa do počítačovej siete a používa zdieľané súbory, databázy, aplikácie, tlačiarne, či iné zariadenia podľa práv, ktoré mu boli pridelené na základe požiadavky, potvrdenej jeho priamym nadriadeným, vedúcim výpočtového strediska súčasti STU, resp. vedúcim zamestnancom, alebo riaditeľom Centra výpočtovej techniky STU.
3. Je preukázateľne poučený o povinnosti dodržiavať Smernicu a Metodické usmernenie a riadiť sa nimi pri svojej práci.
4. Riadi sa pokynmi zamestnancov Výpočtového strediska súčasti STU a CVT STU a obracia sa na nich v prípade závad, porúch a mimoriadnych situácií.
5. Dbá na ochranu spracovávaných dát.
6. PC a ostatné zariadenia IT používa výhradne na služobné účely vyplývajúce z jeho opisu pracovnej činnosti. Na iné účely použitia zariadení IT potrebuje písomný súhlas priameho nadriadeného.

3. Používateľ Internetu

Zamestnanec a študent STU, ktorému bolo pridelené používateľské konto a na základe toho umožnený prístup do celosvetovej počítačovej siete Internet, ako aj iný používateľ z cudzej akademickej inštitúcie autentifikovaný prostredníctvom siete Eduroam.

4. Používateľ Intranetu

Zamestnanec a študent STU, ktorému bolo pridelené používateľské konto a na základe toho umožnený prístup do Intranetu počítačovej siete STU.

4.1 Používateľ elektronickej pošty

Zamestnanec a študent STU, ktorému bolo pridelené používateľské konto a na základe toho umožnené používanie elektronickej pošty (e-mailu).

4.2 Zamestnanec

Pre účely tohto Metodického usmernenia sa za zamestnanca považujú všetci kmeňoví zamestnanci STU a aj externí zamestnanci, ktorí majú s STU pracovno-právny vzťah, prípadne iný zmluvný vzťah.

4.3 Študent

Pre účely tohto Metodického usmernenia sa za študenta považujú študenti všetkých stupňov - bakalárskeho, inžinierskeho a doktorandského, a foriem a to tak dennej ako aj externej formy štúdia na STU.

5. Pravidlá správy a prevádzky dátovej siete STUNET

5.1 Základné ustanovenie

1. Dátová sieť Slovenskej technickej univerzity v Bratislave (STUNET) je súčasťou metropolitnej dátovej siete v Bratislave. Je priamo pripojená na Slovenskú akademickú dátovú sieť pre vedu, výskum a vzdelávanie (SANET) a jej prostredníctvom do európskej vysokorýchlostnej dátovej siete pre vedu výskum a vzdelávanie GEANT a medzinárodnej dátovej siete Internet.
2. Pod pojmom dátová sieť STUNET sa pre účely aplikácie týchto pravidiel považujú všetky technické a programové prostriedky, slúžiace k prepojeniu počítačov, ako aj prostriedky k využitiu tohto pripojenia. Poslaním dátovej siete STUNET je vzájomné prepojenie objektov Slovenskej technickej univerzity v Bratislave a Trnave a ich pripojenie do metropolitnej siete v Bratislave pre zabezpečenie výučby, výskumu a prevádzky školy:
    - Metropolitná chrbticová sieť je časť dátovej siete, ktorá prepája objekty STU v Bratislave a v Trnave s objektmi vysokých škôl v Bratislave, pracoviskami SAV a Ministerstvom školstva, výskumu, vývoja a mládeže SR.
    - Chrbticová sieť STU - STUNET je časť metropolitnej siete, ktorá prepája vstupné prípojné miesto areálu STU s prípojnými miestami lokálnych sietí fakúlt a súčastí (napr. študentský domov) STU
    - Lokálna sieť fakulty alebo súčasti STU je časť dátovej siete STUNET, ktorá zahŕňa koncové zariadenia (používateľské pracovné stanice, servery, tlačiarne a ďalšie zariadenia) a ktorá prepája tieto zariadenia s prípojným miestnom lokálnej siete v rámci areálu i medzi sebou navzájom.

- Server je obslužný počítač (resp. program), ktorý poskytuje presne stanovené služby alebo prostriedky (zdroje) používateľov.
- Sieťová aplikácia je program, ktorý pracuje pre užívateľa a ktorý používateľovi poskytuje vopred stanovené sieťové služby.
- Sieťová služba je služba na zabezpečenie stanovených požiadaviek alebo potrieb používateľov.

Pravidlá uvedené v tomto Metodickom usmernení sú záväzné pre správcov dátovej siete STUNET. Tieto pravidlá sú rovnako záväzné pre používateľov, ktorí spravujú samostatne svoje výpočtové prostriedky napojené na dátovú sieť STUNET.

3. Správca dátovej siete STUNET je osoba zodpovedná za prevádzku konkrétnej dátovej siete, jej častí alebo sieťovej aplikácie.

5.2 Prístupové práva a identifikácia užívateľov

1. Dátovú sieť STUNET môžu využívať len oprávnení používatelia. Oprávnenými používateľmi (ďalej len používateľ) sú používatelia, ktorí boli preukázateľne oboznámení s týmto usmernením. Aktuálny zoznam používateľov dátovej siete s IP adresami zariadení a využívaní doménového priestoru udržuje správca dátovej siete, alebo jej časti.
2. Oprávnenie používať prostriedky dátovej STUNET majú zamestnanci a študenti STU. Používanie dátovej siete STUNET osobami iných organizácií, je možné len na základe písomného povolenia vydaného rektorom STU, dekanom, alebo vedúcim zamestnancom súčasti STU. Takéto povolenie sa vzťahuje len na používanie siete STUNET a neplatí automaticky aj na používanie Slovenskej akademickej dátovej siete SANET. (STU nemá právo predávať ani umožňovať prístup do siete SANET iným organizáciám. Toto právo prislúcha len Združeniu SANET prostredníctvom svojej správy uzlov).
3. Pokiaľ je pre prístup k dátovej siete STUNET požadovaná identifikácia používateľa, je používateľ povinný používať meno pridelené správcom dátovej siete STUNET. Používateľ je povinný používať pre overenie identity heslo, vytvorené na základe pravidiel, udržovať toto heslo v tajnosti, tak aby bolo zabránené jeho zneužitiu.
4. Používateľ nesmie poskytnúť pridelené meno a heslo inej osobe. Za hrubé porušenie pravidiel sa považuje poskytnutie mena a hesla osobe, ktorá nemá nárok na prístup do siete, alebo ktorej bol prístup odopretý alebo zablokovaný.
5. Používateľ nesmie zneužiť nedbanlivého správania iného používateľa, (napr. náhodné zistenie mena a hesla, zabudnuté odhlásenie a pod.) k tomu, aby pracoval pod iným – cudzím menom a heslom.
6. Prístupové práva používateľa sú pridelené správcom dátovej siete. Používateľ sa nesmie žiadnymi prostriedkami pokúsiť získať prístupové práva, ktoré mu neboli pridelené. Pokiaľ používateľ získa prístupové práva neoprávnene bez vlastného pričinenia, napr. chybou systému, je povinný túto skutočnosť bezodkladne ohlásiť správcovi súčasti dátovej siete (na úrovni katedry, ústavu, objektu fakulty) na

adresu **spravca.xxxxxx@stuba.sk** (napr. spravca.cvtstu@stuba.sk) alebo na adresu **it.security@stuba.sk** a tieto práva nesmie použiť.

7. Používateľ sa dopustí hrubého porušenia disciplíny pokiaľ sa pokúsi zneužiť dátovú sieť STUNET k získaniu neautorizovaných prístupových práv k ľubovoľným informačným zdrojom dostupným prostredníctvom dátovej siete STUNET, pokiaľ podnikne cez sieť STUNET softvérové útoky na počítače a iné zariadenia kdekoľvek v sieti Internet.

5.3 Organizačná štruktúra správy dátovej siete STUNET

1. Dátová sieť má hierarchickú štruktúru. Člení sa na:
    a) chrbticovú sieť
    b) lokálnu sieť fakúlt a súčastí STU
    c) sieťové aplikácie
2. Správu chrbticovej siete, vrátane prípojných miest do akademickej siete SANET, medzinárodných sietí GEANT (európskej vysokorýchlostnej dátovej siete pre vedu výskum a vzdelávanie) a medzinárodnej siete Internet a celouniverzitných sieťových aplikácií zabezpečuje Centrum výpočtovej techniky STU. Správu chrbticovej siete areálov STU, správu lokálnych sietí fakúlt a súčastí STU a správu lokálnych sieťových aplikácií, zabezpečujú príslušní správcovia siete súčastí STU.
3. Prevádzku centrálnych informačných systémov a centralizovanej výpočtovej techniky zabezpečuje Centrum výpočtovej techniky STU. Jeho poslanie a pôsobnosť vymedzuje organizačný poriadok STU a Organizačný poriadok CVT STU.
4. Správcovia študentských dátových sietí na študentských domovoch a jedálňach sú podriadení správcovi chrbticovej siete STU a na vyššej úrovni riaditeľovi Centra výpočtovej techniky STU.
5. **Zoznam správcov jednotlivých súčasti siete STUNET musí byť verejne dostupný a aktuálny na www stránke CVT STU.**

5.4 Práva a povinnosti správcov dátovej site STUNET

1. Správca lokálnej sieťovej aplikácie a lokálnych serverov:
    a) zabezpečuje prevádzku sieťovej aplikácie (inštalácia, úpravy, konfigurácia, zálohovanie dát a pod.)
    b) vytvára používateľské kontá podľa zásad platných pre konkrétnu lokálnu sieťovú aplikáciu a prideľuje používateľom prístupové práva
    c) zodpovedá za bezpečné uloženie záložných dát, rieši havarijné stavy
2. Správca lokálnej siete fakulty a súčasti STU:
    a) zabezpečuje prevádzku lokálnej siete od prípojného miesta chrbticovej siete areálu až ku koncovým používateľským pracovným staniciam
    b) zabezpečuje správnu funkciu lokálnych serverov

c) vytvára a spravuje používateľské kontá podľa zásad platných pre prevádzku lokálnej dátovej siete a prideľuje používateľom prístupové práva
d) udržuje konfiguráciu systémov pre počítače, ktorých systém je spúšťaný zo servera
e) prideľuje IP adresy zariadeniam z rozsahu IP adries, ktoré má v správe
f) udržuje aktuálny zoznam MAC a IP adries všetkých pripojených zariadení a všetky zmeny hlási správcovi lokálnej siete fakulty
g) spravuje príslušný doménový priestor fakulty, alebo súčasti
h) informuje používateľov o pravidlách práce v sieti
i) zodpovedá za bezpečné uloženie záložných dát, rieši havarijné stavy

3. Správca chrbticovej siete STU:
   a) zabezpečuje prevádzku chrbticovej siete
   b) zabezpečuje pre STUNET konektivitu pripojených dátových sietí
   c) uskutočňuje pravidelné monitorovanie chrbticovej siete
   d) zabezpečuje prevádzku centrálnych serverov
   e) poskytuje odborné konzultácie vedeniu školy
   f) sleduje vývojové trendy v oblasti dátových sietí a navrhuje spôsob ich implementácie do siete STUNET
   g) organizuje zavádzanie nových sieťových služieb
   h) poskytuje odborné konzultácie správcom podriadených sietí
   i) riadi správu doménového priestoru stuba.sk
   j) usmerňuje a konzultuje podmienky registrácie domén prvej úrovne xxx.sk pre prevádzku v sieti STUNET.
4. Správca siete na všetkých úrovniach najmä:
   a) zabezpečuje prevádzku siete, servera alebo sieťovej aplikácie
   b) kontroluje dodržiavanie pravidiel prevádzky siete
   c) monitoruje prevádzku siete a rieši prípadné kolízie
   d) zálohuje a archivuje dáta na spravovaných zariadeniach

5.5 Používanie dátovej siete STUNET

1. Používateľ môže používať výpočtové prostriedky a dátovú sieť STUNET výlučne pre vedecké, výskumné, vzdelávacie, vývojové a umelecké účely, alebo úlohy súvisiace s prevádzkou, riadením a správou STU. Za porušenie pravidiel sa považuje najmä použitie siete pre komerčnú činnosť nesúvisiacu s činnosťou STU, ďalej šírenie obchodných a reklamných informácií, politickú, náboženskú alebo rasovú agitáciu, propagáciu násilia, drog a šírenie takých materiálov, ktoré sú v rozpore so zákonom.
2. Používateľ má právo používať výlučne legálne nadobudnuté programové vybavenie. Kopírovať programy je možné pri dodržaní platných autorských zákonov. Voľne dostupné programové produkty a informačné materiály, získané s pomocou dátovej siete STUNET smie používateľ používať výlučne pre účely

uvedené v odst. 1. Za hrubé porušenie pravidiel je považované použitie dátovej siete STUNET na ponuku nelegálne získaného programového vybavenia, informačných materiálov, umeleckých alebo literárnych diel a dát.

3. Používateľ nesmie zasahovať do žiadnych programových produktov, dát, systémového a technického prostredia dátovej siete STUNET bez výlučného súhlasu správcu siete. Zvlášť prísne zakázané sú neautorizované zmeny konfigurácie počítačov alebo iných prostriedkov, ktoré by mohli mať vplyv na správnu prevádzku dátovej siete STUNET. Študenti ako používatelia dátovej siete nie sú oprávnení inštalovať akékoľvek programy v dátovej sieti bez výslovného súhlasu správcu siete.
4. Používateľ má právo používať vyčlenený diskový priestor, výpočtové prostriedky a dátovú sieť STUNET len pri zohľadnení jej celkového zaťaženia. Používateľ nesmie vedome narušiť činnosť výpočtových prostriedkov, obmedziť prácu ďalších používateľov, ani chod a výkonnosť siete. Musí bezodkladne vykonať pokyny správcu dátovej siete na zníženie záťaže, ktorú generuje do siete.
5. Veľkosť posielanej elektronickej pošty a konferencií môže byť v dátovej sieti STUNET obmedzená. Konkrétny limit veľkosti elektronickej pošty je stanovený technickým vybavením siete a určuje ho správca siete STUNET. Pri prekročení používateľského limitu využívaného diskového priestoru môže dôjsť k automatickému zablokovaniu príjmu pošty pre konkrétneho používateľa.
6. STU nezodpovedá za stratu používateľských dát a obsahu informácií, ktorá vznikla akýmkoľvek spôsobom v sieti STUNET. Za vytváranie záložných kópií používateľských programov a informačných dát zodpovedajú používatelia sami.
7. Používateľ nesmie ďalej používať počítač, ktorý je napadnutý vírusom a informoval ho o tom antivírový program alebo iný používateľ. Je povinný okamžite vykonať kroky na jeho odvírenie, resp. zničenie škodlivých programov alebo odpojenie zo siete do príchodu správcu siete alebo ním povereného technika siete STUNET.
8. Slovenská technická univerzita je členom Združenia slovenskej akademickej dátovej siete SANET a sieť STUNET je priamo pripojená do tejto siete, preto všetci používatelia siete STUNET sú povinní dodržiavať „Všeobecné pravidlá používania siete SANET“.

5.6 Pravidlá pre pripojenie k dátovej sieti STUNET

1. Používateľ dátovej siete STUNET je povinný požiadať o súhlas správcu lokálnej siete fakulty alebo súčasti STU:
    a) pred pripojením každého nového zariadenia na dátovú sieť
    b) pred zmenou konfigurácie zariadenia, ktorá by mohla mať vplyv na bezporuchovú prevádzku siete
    c) pred trvalým odpojením zariadenia od dátovej siete
2. Správca siete STUNET zaregistruje prípojné zariadenia podľa pravidiel správy dátovej siete STUNET v Bratislave a pridelí pripojenému zariadenie IP adresu.

3. Za správnu inštaláciu operačného systému a sieťového programového vybavenia počítačov, pripojených k dátovej sieti STUNET zodpovedá poverený zamestnanec, určený správcom siete alebo používateľ pokiaľ mu správca siete povolil inštalovať operačný systém samostatne.
4. Pri samostatnej správe operačného systému a sieťového programového vybavenia počítača pripojeného do dátovej siete musí používateľ dodržiavať príslušné pokyny správcu site na príslušnej úrovni.
5. Používateľ nesmie používať pre pripojenie k dátovej sieti inú sieťovú adresu než mu bola pridelená (automatické alebo statické pridelenie adresy).

6. Pravidlá na používanie prostriedkov IT

6.1 Používanie hardvéru

1. Na pracoviskách STU sa používa iba taký hardvér, ktorý je schválený príslušnými vedúcimi VS súčastí STU, riaditeľom CVT STU a je evidovaný v evidencii majetku na oddelení správy majetku súčastí STU ako HIM alebo DIM.
2. Používanie vlastných zariadení (BYOD – Bring Your Own Device) na prístup k sieti STUNET a jej aplikáciám je povolené len na základe predchádzajúceho schválenia IT útvarom a po absolvovaní školenia IT bezpečnosti. Zamestnanci sú povinní zabezpečiť svoje zariadenia silným heslom, pravidelne ich aktualizovať a používať schválený antivírusový softvér, a sú povinný umožniť monitorovanie splnenia týchto povinností IT útvarom príslušnej súčasti STU. Prístup BYOD zariadení k sieti Intranet je možný výhradne cez zabezpečené pripojenie (VPN STUNET). Je zakázané uchovávať citlivé údaje na zariadení bez šifrovania.
3. Akýkoľvek iný hardvér sa zakazuje používať.
4. Zakazuje sa akýkoľvek zásah do hardvéru alebo jeho konfigurácie a jeho svojvoľné premiestňovanie či výmena. Touto činnosťou je poverený technik príslušného IT útvaru súčasti STU alebo CVT STU, ktorý túto činnosť vykoná na základe schválenej požiadavky.
5. Pri presune, sťahovaní či výmene treba požiadať o prevedenie a zaregistrovanie zmeny v evidencii majetku oddelenie správy majetku súčasti STU.
6. Používatelia IT, ktorým boli zverené či zapožičané prenosné notebooky, či akékoľvek iné zariadenia IT, sú povinní používať ich tak, aby nedošlo k ich strate, zneužitiu či krádeži, a nesmú ich požičať, prenechať, odovzdať tretej osobe, či u tretej osoby takéto zariadenie založiť formou záložného práva. V prípade potreby požičania zvereného IT zariadenia inej osobe musí používateľ IT zariadenia požiadať o písomný súhlas príslušného vedúceho zamestnanca STU. Dôverné údaje uložené na disku notebooku musia byť zašifrované a šifrovací kľúč musí byť uložený mimo notebook (napríklad na USB kľúči).

7. Poruchu hardvéru treba nahlásiť príslušnému IT útvaru súčasti STU, alebo CVT STU formou požiadavky. Zamestnanci IT útvaru súčasti STU sa bezodkladne, prípadne podľa dohody postarajú o odstránenie, nápravu, opravu či výmenu.

6.2 Používanie softvéru

1. Pri práci s PC je zakázané pracovať s iným softvérom, než aký bol nainštalovaný, resp. schválený IT útvarom súčasti STU.
2. Používateľ IT používa len ten softvér, na ktorého používanie má podľa schválenej požiadavky právo.
3. Pri akejkoľvek zmene týkajúcej sa používateľa IT majúcej vplyv na používanie softvéru je povinný jeho priamy nadriadený formou požiadavky požiadať o vykonanie tejto zmeny príslušný IT útvar.
4. Po zakúpení softvéru tento nový softvér inštalujú zamestnanci príslušného IT útvaru súčasti STU alebo zamestnanci dodávateľskej firmy za prítomnosti zamestnanca príslušného IT útvaru a oddelenie správy majetku má povinnosť tento softvér zaevidovať.
5. Poruchu softvéru treba nahlásiť príslušnému IT útvaru súčasti STU formou požiadavky. Pracovníci IT útvaru súčasti STU sa bezodkladne, prípadne podľa dohody postarajú o odstránenie, nápravu, opravu či výmenu.
6. Zakazuje sa používať, uchovávať, distribuovať akýkoľvek pirátsky softvér a údaje na hardvérovom vybavení STU.
7. Na inštalovanom hardvérovom vybavení STU je nevyhnutné dôsledne pravidelne kontrolovať aktuálnosť a platnosť inštalovaných opráv (patch) odporúčaných výrobcom a v prípade ich neaktuálnosti požadovať ich aktualizáciu.

6.3 Používanie Internetu, Intranetu a elektronickej pošty

1. Na elektronickú poštu zamestnanca STU oprávneného používať prostriedky siete STUNET, je treba nahliadať ako na neverejnú komunikáciu medzi jednotlivými subjektami pripojenými do siete, na ktorú sa vzťahuje poštové tajomstvo v zmysle príslušného zákona. Pre zaistenie bezpečnosti a kontinuity prevádzky IS a siete STUNET, ako aj v prípade požiadavky na súčinnosť orgánom činným v trestnom konaní, má STU právo v súčinnosti s orgánmi činnými v trestnom konaní, alebo v internom priestupkovom konaní podľa interných predpisov STU na prístup k záznamom elektronickej pošty a právo preveriť prístup zamestnanca a študenta do IS a do siete STUNET.
2. Zobrazenie, archivovanie, uchovávanie, rozširovanie, spracovávanie alebo zaznamenávanie akéhokoľvek obrázku, či dokumentu s jednoznačným sexuálnym obsahom v ktoromkoľvek počítačovom systéme STU sa zakazuje.
3. Prístup na Internet a elektronickú poštu sa nesmie vedome použiť na porušenie zákonov, predpisov a legislatívy SR, či iných štátov.

4. Akýkoľvek softvér alebo súbory, dokumenty, získaný prostredníctvom Internetu a uložený na počítači lokálnej siete súčasti STU, sa môžu používať výhradne len spôsobom, ktorý je v súlade s ich licenciami, autorskými právami, po odsúhlasení zamestnancami IT útvaru súčasti STU a musia priamo súvisieť s pracovnými povinnosťami používateľa IT.
5. Zakazuje sa získavanie a následné ukladanie zábavného softvéru alebo hier, videí, obrázkov a zvukových súborov z Internetu alebo prostredníctvom elektronickej pošty, hranie hier na Internete a prostredníctvom neho. Takisto sa zakazuje rozširovanie akéhokoľvek softvéru či údajov, ktoré sú majetkom STU.
6. Používateľom Internetu a elektronickej pošty na STU sa zakazuje využívať svetovú počítačovú sieť Internet a elektronickú poštu na zámerné rozširovanie akýchkoľvek vírusov, červíkov, trójskych koňov alebo iného škodlivého softvéru. Takisto používateľ nesmie využiť či zneužiť prístup na Internet či elektronickú poštu na vyradenie, preťaženie alebo oklamanie akéhokoľvek počítačového systému alebo počítačovej siete, a tým narušiť súkromie alebo bezpečnosť iného používateľa či spoločnosti.
7. Každý používateľ Internetu a elektronickej pošty sa bude identifikovať svojim menom, prípadne pracovným zaradením, alebo u študentov STU fakultou a katedrou, na ktorej študuje, ak sa to vyžaduje.
8. Hovoriť, písať a prispievať v mene STU, alebo jej súčasti do akýchkoľvek diskusných skupín môžu len zamestnanci STU, ktorí sú riadne poverení komunikáciou s médiami. Ostatní používatelia Internetu a elektronickej pošty sa môžu zúčastňovať na diskusiách a fórach v priebehu pracovnej doby, ak sa to vzťahuje na ich odbornú činnosť, ale v tom prípade vystupujú ako jednotlivci vo vlastnom mene a sú povinní informovať ostatných zúčastnených, že nie sú oprávnení vystupovať v mene STU, alebo jej súčasti. Pri účasti v týchto diskusiách a fórach je používateľ Internetu a elektronickej pošty povinný zdržať sa akýchkoľvek politických, náboženských, rasových prejavov, prejavov neznášanlivosti a prejavov urážajúcich ľudskú dôstojnosť, či prejavov týkajúcich sa trestnej činnosti a zverejňovať údaje a dôverné informácie STU.
9. Používatelia Internetu a elektronickej pošty môžu využívať prístup na Internet a elektronickú poštu pre prieskum alebo prezeranie informačných zdrojov nesúvisiaci s pracovnou náplňou počas obedovej alebo inej prestávky, alebo po pracovnej dobe, ale za predpokladu, že budú dodržané všetky ustanovenia tejto smernice.
10. STU je povinná poskytnúť orgánom činným v trestnom konaní všetky dostupné záznamy, týkajúce sa prístupu na Internet a elektronickú poštu príslušného používateľa Internetu a elektronickej pošty podľa príslušných zákonných ustanovení.

11. Používateľ Internetu a elektronickej pošty musí porozumieť a riadiť sa právnymi predpismi, autorským právom, obchodnými značkami. V tomto je používateľom Internetu a elektronickej pošty nápomocné právne oddelenie STU.
12. Komerčné používanie Internetu na podporu vedľajšej podnikateľskej činnosti zamestnanca STU alebo jej súčasti mimo jeho pracovnej náplne je možné iba na základe podmienok stanovených v zmluve, uzavretej medzi STU a Združením používateľov slovenskej akademickej dátovej siete - SANET, prevádzkujúcim pripojenie siete STU do medzinárodnej siete Internet.

6.4 Používanie hlasovej, faxovej a obrazovej komunikácie pri posielaní osobných údajov alebo iných citlivých informácií

1. Používanie hlasovej, faxovej a obrazovej komunikácie na STU pri posielaní osobných údajov alebo iných citlivých informácií sa riadi smernicou rektora **„Klasifikácia aktív informácií informačného systému STU“**.
2. Každý vlastník aktív informačného systému je povinný dodržiavať pri používaní hlasovej, faxovej a obrazovej komunikácie vyššie uvedenú smernicu s tým, že každé porušenie ustanovení tejto smernice bude chápané ako porušenie pracovnej disciplíny v zmysle pracovného poriadku.
3. Každý vlastník aktív informačného systému zabezpečí, aby posielanie osobných údajov a citlivých informácií mohli vykonávať len písomne poverené osoby na základe zaškolenia. O poverení a zaškolení vedie evidenciu vlastník aktív.
4. Všetky zariadenia slúžiace na zber, archivovanie a posielanie citlivých informácií informačného systému sa musia využívať v súlade s pridelenými oprávneniami na základe Smernice a tohto Metodického usmernenia. Toto ustanovenie zahŕňa aj dodržiavanie povinností informovať administrátora IT a správcu lokálnej siete súčasti STU o prípadných zmenách pôvodne nastavených funkcionalít zariadení IT a o bezpečnostných incidentoch.
5. Rektor, dekani fakúlt, a ostatní vedúci zamestnanci súčastí STU zabezpečia pri nástupe nového zamestnanca jeho vstupné zaškolenie na používanie informačného systému, vrátane ochrany a bezpečnosti prístupu. Absolvovanie vstupného zaškolenia musí byť dokumentované a archivované na príslušnom personálnom útvare fakulty alebo súčasti STU.
6. Vedúci zamestnanci fakúlt a ostatných súčastí STU zabezpečia preškolenie zamestnancov v zmysle tohto Metodického usmernenia ako súčasť preškolenia „Bezpečnosti pri práci“ s pravidelnou minimálne 3-ročnou periodicitou vrátane vyhotovenia príslušných protokolov o vykonaní preškolenia.

6.5 Kamerové systémy

1. STU má právo používať na monitorovanie svojich vnútorných priestorov a na prístupových komunikáciách kamerové systémy, z dôvodov zabezpečenia ochrany majetku a osôb.
2. Na všetkých priestoroch, ktoré sú monitorované kamerovým systémom musí byť označenie na viditeľnom mieste označenie „Priestor je monitorovaný kamerovým systémom“.
3. Záznamy sa aktuálne zapisujú na pamäťové médium a v lehote 3 dní (72 hodín) musia byť z archívu priebežne mazané.
4. Prístup k archívnym záznamom a tiež k on-line monitoru majú len oprávnené osoby.
5. Kamerové systémy nesmú byť použité na monitorovanie osôb pri pracovnej činnosti, príchodu a odchodu do práce ako aj pri ostatných bežných činnostiach na pracovisku.

7. Pravidlá pre autentifikáciu používateľov

7.1 Heslo administrátora

1. Heslo musí byť menené pravidelne, v intervaloch medzi jednotlivými zmenami max. 90 dní.
2. Heslo musí mať najmenej 12 znakov, pričom v hesle môžu byť použité písmená anglickej abecedy, číslice a špeciálne znaky ,?.:-_!/|\=+[(]). V hesle musí byť použitý najmenej jeden znak z intervalu A ... Z, aspoň jeden znak z intervalu a ... z a aspoň jedna číslica.
3. Posledných 5 použitých hesiel musí byť vzájomne rôznych.
4. Bezpečnostná kópia aktuálneho hesla administrátora musí byť zapísaná a uložená v zalepenej zapečatenej obálke u riaditeľa CVT STU.

7.2 Heslá používateľov s privilegovaným prístupom

Používatelia „správca DBS ORACLE, DBS Microsoft SQL“, „správca OS Unix, OS MS Windows“ a pod. :

1. Heslo musí byť menené pravidelne, v intervaloch medzi jednotlivými zmenami max. 90 dní.
2. Heslo musí mať najmenej 12 znakov, pričom v hesle môžu byť použité písmená anglickej abecedy, číslice a špeciálne znaky ,?.:-_!/|\=+[(]). V hesle musí byť použitý najmenej jeden znak z intervalu A ... Z, aspoň jeden znak z intervalu a ... z a aspoň jedna číslica.
3. Posledných 5 použitých hesiel musí byť vzájomne rôznych.

4. Po piatom zadaní nesprávneho hesla musí systém zamknúť daný používateľský účet.

7.3 Heslá ostatných používateľov

IT útvary súčasti STU a CVT STU musí evidovať v písomnej forme a archivovať údaje o zriadených používateľských účtoch, napríklad v **Denníku používateľských účtov a prístupových práv**. Oprávnenosť existencie používateľského účtu musí byť v pravidelných intervaloch (2×ročne) preverovaná.

1. Heslo musí byť menené pravidelne, v intervaloch medzi jednotlivými zmenami max. 180 dní.
2. Heslo musí mať najmenej 12 znakov, pričom v hesle môžu byť použité písmená anglickej abecedy, číslice a špeciálne znaky ,?.:-_!/|\=+[(]). V hesle musí byť použitý najmenej jeden znak z intervalu A ... Z, aspoň jeden znak z intervalu a ... z a aspoň jedna číslica.
3. Ako heslá sa nesmú používať slová a čísla, ktoré sú spojené s používateľom (jeho meno, dátum narodenia, tel. číslo a pod.).
4. Ak je heslo priradené administrátorom (pri vytvorení účtu, resp. pri zabudnutí hesla používateľom), po prvom prihlásení používateľa musí systém vynútiť zadanie nového používateľského hesla.
5. Posledných 5 použitých hesiel musí byť vzájomne rôznych.

7.4 Prideľovanie adries elektronickej pošty

1. Adresy elektronickej pošty v tvare meno.priezvisko@stuba.sk a prístupové heslá zamestnancov prideľuje pri nástupe do zamestnania pracovník personálneho oddelenia súčasti STU.
2. Pri ukončení pracovného pomeru sa adresa elektronickej pošty a prístupové heslo zamestnanca zablokuje po uplynutí 180 dní.
3. Študentom I. ročníka pri zápise odovzdá automaticky vygenerovanú adresu xxxxxx@stuba.sk elektronickej pošty a prístupové heslo zamestnanec študijného oddelenia dekanátu príslušnej fakulty.
4. Pri prerušení alebo ukončení štúdia sa adresa elektronickej pošty a prístupové heslo zablokuje po uplynutí 180 dní.
5. Pri novom nástupe po prerušení štúdia študent požiada o znovu pridelenie adresy elektronickej pošty a prístupového hesla študijné oddelenie príslušnej fakulty.
6. Pri strate prístupového hesla môže študent požiadať o jeho vydanie zamestnanca študijného oddelenia fakulty.

7.5 Prideľovanie prístupových hesiel do Informačného systému

1. Prístupové heslá do EIS Magion prideľujú správcovia jednotlivých modulov na základe písomnej žiadosti príslušného nadriadeného vedúceho zamestnanca

rektorátu, fakúlt a súčastí STU, zamestnanca pre ktorého sa vytvára prístup do EIS. Zoznam správcov EIS je v prílohe tohto Metodického usmernenia.

2. Pridelené heslo slúži na prvotné prihlásenie a po aktivovaní prístupu je používateľ na výzvu systému povinný si heslo zmeniť na základe pravidiel uvedených v čl. 7.3.
3. Po ukončení pracovného pomeru sa heslo automaticky zmaže.
4. Prístup k jednotlivým modulom EIS Magion je možný len zo siete STUNET, alebo cez VPN STUNET.
5. Prístupové heslá do AIS prideľujú integrátori systému, personálne, a študijné oddelenia na fakultách a správca systému CVT STU. Pridelené heslo súži aj na prístup do elektronickej pošty, stravovacieho systému KREDIT, do knižničného systému ARL. Platnosť hesla overujú tieto systémy prostredníctvom služby LDAP. Zoznam integrátorov AIS je v prílohe tohto Metodického usmernenia.
6. Po ukončení pracovného pomeru alebo štúdia je prístup do informačného systému AIS možný cez ID používateľa nepretržite s obmedzenými funkcionalitami.
7. Pre zaručenie vyššej úrovne bezpečnosti prístupu a ochrany dát v AIS majú učitelia a doktorandi prístup k „Zápisníku učiteľa a výskumníka“ cez ďalší stupeň autentifikácie a to prostredníctvom „Preukazu zamestnanca“ s čipom, ku ktorému je pridelený certifikát certifikačnou autoritou IS STU (pozri Smernica rektora č. 3/2016-SR Zvýšenie bezpečnosti AIS STU a Certifikačný poriadok IS STU Bratislava CA 1.0.), alebo pomocou jednorazových TOTP kódov prostredníctvom mobilnej aplikácie Authenticator.
8. Prístup do dochádzkového systému (EDS) prideľuje správca systému. Prihlasovacím menom je osobné číslo zamestnanca, prvotné heslo je rovnaké, systém po prihlásení žiada heslo zmeniť. Systém umožňuje nastaviť aj vyššiu úroveň prístupu umožňujúcu prezerať a prípadne aj editovať dochádzku podriadených zamestnancov. Toto právo prideľuje na základe žiadosti nadriadeného zamestnanca správca EDS. Zoznam správcov je v prílohe tohto Metodického usmernenia.

7.6 Prideľovanie hesiel pre vzdialený VPN prístup do WIFI siete

1. Heslá sú vytvárané aplikačne v príslušnej používateľskej sekcii v informačnom systéme AIS.
2. Heslá nie sú zhodné s heslami na prístup do informačných systémov.
3. Po ukončení pracovného pomeru alebo štúdia sa heslo automaticky zablokuje.

7.7 Používanie viacfaktorového overovania

1. Administrátori a používatelia s privilegovaným prístupom sú povinný používať viacfaktorové overovanie (MFA) vo všetkých systémoch, ktoré to umožňujú. Ostatným používateľom sa používanie MFA dôrazne odporúča.
2. Používajú sa nasledovné MFA metódy:

a) Hardvérové bezpečnostné kľúče (FIDO2)
b) Push notifikácie v mobilnej aplikácii Authenticator
c) Jednorazové kódy generované aplikáciou Authenticator (TOTP)
d) Certifikát uložený na čipovej karte alebo inom bezpečnom zariadení

3. Používateľ musí mať vytvorené a bezpečne uložené záložné bezpečnostné kódy alebo ďalšie MFA zariadenie pre prípad nedostupnosti primárneho zariadenia.
4. O odobratie alebo resetovanie MFA metódy môže používateľ príslušného správcu aplikácie žiadať iba vo vlastnom mene a jeho požiadavka musí byť hodnoverne autentifikovaná.

8. Pravidlá riadenia prístupu k aktívnym prvkom komunikačnej infraštruktúry

1. Aktívne prvky komunikačnej infraštruktúry – smerovače, prepínače, dátové brány (gateways), bezpečnostné brány (firewalls) a pod. – môžu byť prístupné iba autorizovaným oprávneným osobám, správcom chrbticovej siete STU a správcom lokálnych sietí súčastí STU.
2. Nastavovanie alebo zmena parametrov aktívnych prvkov komunikačnej infraštruktúry môže byť vykonávaná prostredníctvom priameho pripojenia nastavovacieho zariadenia (terminálu) na komunikačné rozhranie (port) aktívneho prvku vyhradeného výhradne pre tento účel, alebo vzdialene cez zabezpečenú manažovaciu sieť do ktorej je možný prístup z Internetu len prostredníctvom VPN tunela.
3. Každá zmena v nastavení aktívneho prvku chrbticovej siete STU a fakúlt musí byť evidovaná.

9. Disciplinárny postih študentov za porušenie pravidiel prevádzky dátovej siete STUNET

1. Porušenie pravidiel prevádzky dátovej siete STUNET je považované za porušenie vnútorných predpisov STU a rieši sa disciplinárnym konaním v zmysle čl. 9 a nasl. Disciplinárneho poriadku STU.
2. Podľa čl. 6 citovaného Disciplinárneho poriadku je možné študentovi uložiť trest podmienečného vylúčenia zo štúdia, a za zvlášť závažné porušenie pravidiel môže byť študent až vylúčený zo štúdia.
3. Pri závažnejších porušeniach alebo opakovanom menej závažnom porušení pravidiel môže správca alebo ním poverená osoba vziať študentovi na vopred stanovenú dobu (max. 2 mesiace) oprávnenie voľného používania služieb dátovej siete, okrem organizovanej výučby. Študent má v takomto prípade právo odvolať

sa k dekanovi alebo vedúcemu zamestnancovi súčasti STU. Toto odvolanie nemá odkladný účinok.

4. Pri opakovanom alebo zvlášť závažnom porušení pravidiel sa bude postupovať takto:
    a) Dňom zistenia porušenia pravidiel prevádzky dátovej siete stráca študent právo používať služby dátovej siete.
    b) Celý prípad porušenia pravidiel spolu s dokumentáciou je odovzdaný disciplinárnej komisii príslušnej fakulty STU.
    c) Na základe rokovania disciplinárnej komisie dekan príslušnej fakulty rozhodne o uložení trestu. Trestom môže byť tiež znemožnenie služieb dátovej siete STUNET na stanovenú dobu alebo finančná pokuta. Prípadná trestno-právna zodpovednosť pri porušení pravidiel nie je týmto postupom obmedzená ani vylúčená.
5. Pri závažnom porušení pravidiel, napr. nedovoleným získavaním alebo poskytovaním informačných zdrojov z Internetu, má správca právo odpojiť celú sieť alebo jej časť na 24 hodín na vykonanie opatrení. Pri opakovanom takomto porušení pravidiel sa celý prípad rieši disciplinárnym postihom.

10. Disciplinárny postih zamestnancov za porušenie pravidiel prevádzky dátovej siete STUNET

1. Porušenie ustanovení tohto Metodického usmernenia bude u zamestnancov STU považované za porušenie základných povinností zamestnanca v zmysle čl. 6 Pracovného poriadku STU v súlade s príslušnými ustanoveniami Zákonníka práce, a je možné z neho vyvodiť príslušné pracovno-právne dôsledky vrátane rozviazania pracovného pomeru.
2. Pri zistení porušenia pravidiel prevádzky dátovej siete STUNET, správca siete alebo ním poverená osoba upozorní zamestnanca, ktorý pravidlá porušil na túto skutočnosť. V prípade hrubého porušenia upozorní na porušenie pravidiel príslušného vedúceho zamestnanca súčasti STU.
3. Pri opakovanom porušení pravidiel sa bude postupovať takto:
    a) Dňom zistenia porušenia pravidiel stráca zamestnanec právo používania služieb dátovej siete STUNET.
    b) Celý prípad aj s dokumentáciou je odovzdaný dekanovi príslušnej fakulty STU alebo rektorovi STU v prípade ďalších súčastí STU, a ten rozhodne o pracovno-právnom opatrení alebo finančnej pokute. Prípadná trestno-právna zodpovednosť nie je týmto postupom obmedzená ani vylúčená.

11. Ochrana súkromia a zverejňovanie informácií

1. Pre používanie elektronickej pošty a elektronických konferencií platia rovnaké pravidlá, ako pre užívanie bežnej pošty, pričom elektronická poštová správa má charakter neverejnej (dôvernej) listovej zásielky.
2. Používateľ je povinný dbať na to, aby jeho elektronická pošta bola presne adresovaná a nedochádzalo k nežiadúcemu obťažovaniu ostatných používateľov rozposielaním reťazových listov, alebo listov adresovaných na generátore adries, ktoré sú zhromaždené bez súhlasu adresáta.
3. Používateľ je povinný pri odoslaní elektronickej pošty používať pridelené používateľské meno (meno poštovej schránky). Za hrubé porušenie pravidiel je považované odosielanie listov s falošnou identitou s cieľom zastrašovania, získania neoprávnených informácií alebo podvodu.
4. Príjem elektronickej pošty z adries, ktoré porušujú vyššie uvedené tri ustanovenia 1. – 3. tohto článku môže byť zablokovaný.
5. Pri posielaní dokumentov s osobnými údajmi elektronickou poštou musí byť dokument pred odoslaním zašifrovaný („zaheslovaný“). Táto skutočnosť musí byť príjemcovi správy elektronickej pošty oznámená spolu s informáciou o získaní šifrovacieho kľúča („hesla“). Šifrovanie realizovať alebo natívnymi funkciami textových editorov (PDF alebo MS Office) alebo kompresným programom so šifrovaním (napr. 7-Zip). Ak sa na šifrovanie použije kompresný program so šifrovaním s voľbou šifrovacieho algoritmu, potom musí byť v správe pre príjemcu uvedený aj šifrovací algoritmus.
6. Pri posielaní správy študentom STU správu posielať na adresu elektronickej pošty, ktorú študentovi pridelila STU, a ako šifrovací kľúč („heslo“) použiť rodné číslo študenta bez lomky.
7. Pri posielaní správy iným osobám správu poslať na nimi uvedenú adresu elektronickej pošty, zvolený šifrovací kľúč („heslo“) poslať príjemcovi pošty iným kanálom (napr. správou SMS na mobil). Šifrovací kľúč („heslo”) musí mať aspoň desať znakov vrátane veľkého a malého písmena, špeciálny znak a číslicu. Nesmie obsahovať slová zo slovníka. Ak príjemca správy elektronickej pošty nedisponuje alternatívnym kanálom, potom sa za šifrovací kľúč (“heslo”) zvolí dôverná informácia, ktorá je známa iba odosielateľovi a príjemcovi správy, napríklad číslo pasu, rodné číslo, atď. Krajným a bezpečnostne najhorším riešením je poslať šifrovací kľúč („heslo“) v následnej správe elektronickej pošty.
8. Používateľ nesie plnú právnu zodpovednosť za obsah vlastných verejne dostupných www stránok, iných informačných zdrojov, najmä však za prípadné porušenie autorského zákona pri kopírovaní a rozširovaní cudzích programov, informačných materiálov, umeleckých alebo literárnych diel a dát.
9. Súbory v používateľských adresároch a systémových stránkach elektronickej pošty sú súkromnými dátami ich vlastníkov. Používatelia majú nárok na ochranu

súkromia, a to aj v prípade, keď svoje adresáre nechránia zvláštnou ochranou. Za hrubé porušenie pravidiel je považované vytváranie kópií cudzích dát, informačných materiálov a odposluch prevádzky na dátovej sieti STUNET s cieľom získania obsahu správ, alebo iných informácií.

10. Správca dátovej siete STUNET je oprávnený zamedziť prístup do súborov, ktoré by mohli byť využívané v rozpore s účelom uvedeným v čl. 5.5, prípadne ktoré ohrozujú bezpečnosť systému a dátovej siete (nebezpečné programy, vírusy, nástroje na odpočúvanie prevádzky, nástroje na odpočúvanie mena a hesla a pod.) a ich používateľ je povinný na vyzvanie správcu siete tieto programy bezodkladne odstrániť.
11. Ustanovenie povinne zverejňovanej zmluvy, ktoré obsahuje informáciu, ktorá sa podľa zákona nesprístupňuje (napríklad osobné údaje), sa nezverejňuje. Anonymizuje sa tak, že v elektronickej verzii zmluvy sa nesprístupňované informácie vymažú alebo sa nahradia nevýznamnými znakmi, napríklad znakmi x. Ak sa zverejňuje iba papierová verzia zmluvy, nesprístupňované údaje sa anonymizujú tak, že musia byť bezpečne prekryté, aby nebolo možné tieto údaje po prekrytí zistiť.
12. STU nezodpovedá za prípadné zneužitie dát pri prenose a uchovávaní informácií v dátovej sieti STUNET.
13. Správca dátovej siete STUNET má právo vykonávať všetky úkony nevyhnutné k výkonu svojej funkcie, vrátane prípadnej kontroly prenášaných dát a monitorovania činnosti používateľa v sieti. Pokiaľ používateľ používa pre utajenie informácií šifrovanie, je povinný v prípade pochybnosti o účele použitia v zmysle čl. 5.5 sprístupniť správcovi siete obsah dát.
14. Pre zabezpečenie ochrany súkromia v zmysle ustanovení GDPR a Zákona o OOÚ platia „Podmienky ochrany súkromia“ zverejnené na www.stuba.sk. Tento dokument obsahuje podrobný popis všetkých účelov spracovania a zverejňovania osobných údajov.
15. Pre zabezpečenia podmienky práva na prístup k osobným údajom podľa článku 15 GDPR je zriadené webové sídlo https://is.stuba.sk/. Z tohto sídla môžu študenti a doktorandi zistiť, aké osobné údaje sa o nich spracovávajú a zverejňujú na základe oprávnených alebo verejných záujmov, podľa čl. 6 ods. 1 písm. e a f GDPR, vrátane tých, ku ktorým dali súhlas. Súhlas môžu kedykoľvek odvolať.
16. Na webovom sídle https://is.stuba.sk/ je odkaz na personálny portál zamestnanca, kde zamestnanec môže vidieť, aké osobné údaje sa spracovávajú a zverejňujú, prípadne môže požiadať ich opravu podľa čl. 16 GDPR. Opravu je možné u študenta riešiť cez študijné oddelenie a u zamestnanca cez personálny útvar formou dodatkového vyhlásenia, alebo AIS si študent a zamestnanec môžu opraviť osobné údaje aj sami prostredníctvom svojho autorizovaného prístupu na portál AIS.

12. Účtovateľnosť a auditné záznamy

1. Cieľom účtovateľnosti a vytvárania auditných záznamov je záznam činností používateľov a zmien dôležitých údajov, detekcia, prevencia a potláčanie neregulárnych javov pri vstupe, výstupe a spracovaní údajov.
2. Všetky aplikácie IS a operačné systémy musia produkovať auditné záznamy. Tieto záznamy musia poskytovať informácie, ktoré umožnia neskoršie vyšetrovanie straty alebo neautorizovaných zásahov. Musia obsahovať minimálne záznam o významných zmenách údajov, čas a meno autorizovaného používateľa - pôvodcu zmeny.
3. Všetky súbory s auditnými záznamami musia byť chránené pred neautorizovaným prístupom a zásahom. Musia byť archivované v primeraných intervaloch. Auditné záznamy môžu byť vymazané iba s dvojnásobným autorizovaným súhlasom, riaditeľa CVT STU a bezpečnostného manažéra STU alebo inej k tomu oprávnenej osoby. Proces musí byť vykonaný pod dohľadom administrátora IS.
4. Auditné záznamy obsahujú tieto položky:
    - neúspešné pokusy používateľa o autentifikáciu,
    - prístup a aktivita privilegovaných používateľov,
    - neúspešné pokusy o prístup k údajom a funkciám,
    - zmeny v bezpečnostnom systéme a pridružených riadiacich informáciách,
    - všetky prihlásenia a odhlásenia používateľov so zápisom dátumu a času.
5. Administrátor aplikácie monitoruje a vyhodnocuje auditné záznamy aplikácie, systémový administrátor monitoruje a vyhodnocuje auditné záznamy operačného systému, bezpečnostný manažér IS monitoruje a vyhodnocuje všetky auditné záznamy.
6. Žiadna osoba nesmie mať prístupové práva umožňujúce neautorizovanú zmenu alebo vymazanie auditných záznamov.
7. Vyhodnocovanie auditných záznamov sa vykonáva nástrojom na to určeným (filtre s možnosťou nastavenia podozrivých operácií). Metodici aplikácií IS špecifikujú podozrivé operácie používateľov v aplikácii. Tieto operácie majú charakter nekorektných alebo nebezpečných operácií.

13. Zálohovanie údajov serverov informačného systému

1. Z pohľadu charakteru záloh sa zálohy delia na Operatívne a Bezpečnostné.
2. O vykonávaných činnostiach zálohovania vedie zamestnanec záznamy v **Denníku záloh**, ktorý obsahuje:
    a) Dátum, čas začiatku a ukončenia činnosti.
    b) Označenie zodpovedajúceho záznamového média – napr. mg. pásky DAT, CD ROM, CD RW, DVD alebo adresy diskového poľa.

c) U pások pre kontinuálne zálohovanie logických protokolov čísla protokolov uložených na páske.
d) U pások s operatívnou a bezpečnostnou zálohou databázy číslo logického protokolu, ktoré patrí k danej páske.
e) U pások s operatívnou a bezpečnostnou zálohou binárnych súborov operačného systému a vykonateľných súborov aplikácie označenie diskových priestorov zálohovaných na páske.
f) Miesto uloženia archívnej pásky.
g) Problémy, chyby a poznámky o priebehu zálohy.
h) Podpis zamestnanca.

3. Denník záloh, zálohovacie médiá s operatívnymi zálohami a zálohovacie médiá s bezpečnostnými zálohami záložnej sady A musia byť uložené v protipožiarnom trezore (požiarna odolnosť min. 60 minút a schopnosť ochrany obsahu trezoru voči striekajúcej vode).
4. Protipožiarny trezor musí byť umiestnený v dosahu zamestnanca vykonávajúceho zálohy, protipožiarny trezor musí byť umiestnený bezpečnom priestore chránenom elektronickým zabezpečovacím zariadením.

13.1 Operatívna záloha

Zálohovanie databáz databázového servera Oracle:

1. Denne je automaticky vykonávaný logický backup databázy pomocou exportnej utility databázového servera **Oracle exp**, ktorá vykonáva logickú zálohu databázy, zálohovací skript shellu, ktorý túto utilitu využíva je volaný démonom operačného systému **unix cron**.
2. Exportovaná je celá databáza (**full export**). Denne sú kontrolované log súbory z exportu databázy pre prípad výskytu chýb pri exporte. Výsledný súbor takto vytvorenej zálohy databázy, ktorý vo svojom názve obsahuje názov databázy a dátum vykonania jej zálohy je umiestnený na diskovom zariadení, na ktorom sa nenachádzajú žiadne súbory zálohovaných databáz. Raz za týždeň je takto vyexportovaná databáza uložená na zálohovacie páskové médium.
3. Takýmto spôsobom sú vykonávané aj zálohy databáz systému EIS MAGION, AIS (Akademický informačný systém), ARL (Knižničný informačný systém), Ubytovací systém študentov na ŠD, Stravovací systém Kredit pred a po uzávierke mesiaca, tie sú následne uložené na DVD médium alebo na diskové pole.
4. Dodatočne sa vykonáva záloha databázy pomocou fyzickej zálohy databázových súborov a automatickým archivovaním **online redo log súborov** (databáza pracuje v archive log móde pri ktorom sa odkladajú kópie generovaných redo log súborov), za využitia ktorých je možná obnova databázy z fyzickej zálohy databázových súborov. Databázové súbory sa ukladajú na pásku. Pravidelne sú na pásku zálohované archivované redo log súbory.

13.2 Bezpečnostná záloha

Zálohovanie súborov operačného systému a inštalácie databázového servera:

1. Pravidelne sa vykonáva záloha operačného systému a súborov databázového servera pomocou nástroja **vdump** na pásku.
2. Zálohy vykonávané pri zmenách v rámci operačného systému a súborov databázového servera:
    a) Pri inštalovaní patchov pre databázový server, resp. operačný systém, nových verzií operačného systému a databázového servera, príp. iných zmien v rámci týchto systémov sa vykonáva fyzická záloha databázových súborov jednotlivých databáz, záloha operačného systému a súborov databázového servera.
    b) Po vykonaní zálohy je potrebné vykonať kontrolu záznamu o priebehu archivácie alebo spustiť kontrolu čitateľnosti archívnej pásky príkazom **dd**.
    c) Pre bezpečnostné zálohy sú používané 4 sady archívnych pások, ktoré sa cyklicky menia
3. Zálohovanie verzií aplikácií pri prechode na nové verzie aplikácie
    a) Záloha verzií aplikácií pri prechode na novú verziu aplikácie sa vykoná na CD ROM, CD RW alebo DVD médiá spravidla na klientskom rozhraní.

13.3 Likvidácia archívnych médií

1. Papierové médiá (tlačové výstupy informačného systému a pod.) musia byť likvidované v skartovacích strojoch umožňujúcich aspoň rozrezanie na prúžky so šírkou menšou ako 5 mm.
2. Skartovací stroj musí byť umiestnený v miestnosti (priestore) s inštalovanou veľkokapacitnou tlačiarňou alebo spoločnou sieťovou tlačiarňou.
3. Vyradené magnetické archívne média (diskety, pásky) a iné vyradené dátové médiá (CD-ROM, DVD) je potrebné skartovať (v skartovacom stroji, resp. pod dohľadom rozdrviť alebo fyzicky zlikvidovať v spaľovni odpadu).

13.4 Plán kontinuity činnosti informačného systému STU

1. Pre zabezpečenie kontinuity informačného systému je vypracovaný „**Havarijný plán informačného a počítačového systému STU**“ ako súčasť zabezpečenia ochrany údajov a informačnej bezpečnosti informačného systému STU.
2. Súčasťou tohto havarijného plánu je aj plán obnovy činnosti informačného systému po jeho havárii.
3. Základnou podmienkou obnovy činnosti po havárii je zistiť dôvod havárie, alebo narušenia informačného a počítačového systému STU a zabrániť ďalším poškodeniam zariadení počítačového systému alebo dát.
4. Obnova činnosti havarovaného informačného systému STU podľa stupňa poškodenia je možná na pôvodnom (opravenom) HW alebo na dočasnom HW

pôvodne slúžiacom pre iný účel. STU neplánuje prevádzkovať kompletnú zálohu HW a SW informačného systému, ani neplánuje vytvorenie a inštaláciu záložného informačného počítačového systému v náhradnom prostredí. Rovnako tak STU neplánuje prevádzkovať plne záložný informačný a počítačový systém.

5. Pre zabezpečenie kontinuity informačného systému je nevyhnutné zabezpečiť zálohovanie všetkých relevantných dát informačného systému vrátane aktuálnych databáz.

14. Klasifikácia, označovanie a manipulácia s dokumentami

1. Klasifikácia a označovanie dokumentov obsahujúcich citlivé informácie označované ako dôverné v papierovej aj v elektronickej forme a dokumentov s informáciami pre internú potrebu, ktoré sú zhromažďované, spracovávané a archivované na pracoviskách STU je určená vnútornými predpismi vydanými rektorom STU – Smernicou rektora **„Klasifikácia aktív a informácií informačného systému STU“**, **„Registratúrnym poriadkom STU“** a **„Smernicou na ochranu osobných údajov STU“**.
2. Ostatné dokumenty, ktoré nespadajú do vyššie uvedených kategórií, sú dokumenty verejne prístupné, ktoré nemajú charakter citlivých informácií a je možné ich ľubovoľne zverejňovať, kopírovať a šíriť.

15. Zabezpečenie ochrany osobných údajov pri dodávke, inštalácii a údržbe technických a programových prostriedkov IS

1. Pri uzatváraní dodávateľských zmlúv na dodávku programových systémov, ich inštalácie, alebo na zabezpečenie ich pravidelnej údržby, je vedúci pracovník fakulty alebo súčasti STU povinný zabezpečiť, aby každá takáto zmluva obsahovala článok uvádzajúci povinnosť dodávateľa zachovávať mlčanlivosť pri styku s osobnými údajmi zamestnancov alebo študentov STU v súlade s ustanoveniami §79 Zákona o OOÚ.
2. Rovnaká povinnosť sa týka aj dodávky technických a sieťových zariadení a komponentov. Pri prideľovaní prístupových práv tretím osobám je potrebné postupovať podľa ustanovení Smernice a tohto Metodického usmernenia.
3. Pri uzatváraní kooperačných zmlúv, dohôd o vykonaní práce alebo dohôd o pracovnej činnosti na činnosti vzťahujúce sa k informačnému a komunikačnému systému STU je potrebné postupovať podľa „Smernice na ochranu osobných údajov na STU“.

16. Previerka informácií a zariadení IS

1. Pre zabezpečenie pravidiel pre bezpečnú a spoľahlivú prevádzku a používanie informačného systému STU v súlade s ustanoveniami Smernice a tohto Metodického usmernenia je potrebné vykonávať priebežné kontroly ich plnenia:
    a) raz ročne vykonať previerku zariadení na zber a spracovanie informácií a dokumentov o používaní aktív informačného systému STU v zmysle zhody s bezpečnostným zámerom STU.
    b) raz za 3 roky realizovať externé audity prevádzkovaných informačných systémov. Pod externými auditmi sa rozumie, že audit prevádzkovaných informačných systémov vykoná dodávateľská firma, alebo komisia zložená z odborníkov z radov zamestnancov STU na informačné komunikačné technológie, ktorá nemá v pracovnej náplni zabezpečovať prevádzku informačných systémov.

17. Kontrolná činnosť

Kontrolnú činnosť dodržiavania Smernice a tohto Metodického usmernenia vykonávajú všetci vedúci zamestnanci a všetci vedúci útvarov STU, fakúlt STU a súčastí STU v rámci svojich právomocí a pôsobnosti.

18. Prílohy

18.1 Zoznam správcov modulov IS na pracovisku UIS CVT STU

- https://www.stuba.sk/sk/pracoviska/centrum-vypoctovej-techniky/cinnosti-a-sluzby/prevadzkovanie-informacneho-systemu.html?page_id=1598

18.2 Zoznam integrátorov AIS na fakultách

- https://is.stuba.sk/dok/integratori.pl

18.3 Zoznam správcov siete STUNET

- https://www.stuba.sk/sk/pracoviska/centrum-vypoctovej-techniky/cinnosti-a-sluzby/zoznam-spravcov-siete-stunet.html?page_id=12742

18.4 Helpdesk CVT STU

Helpdesk je centralizované kontaktné miesto Centra výpočtovej techniky STU, kde môžu koncoví používatelia získať technickú podporu, klásť otázky alebo nahlasovať požiadavky a problémy týkajúce sa výpočtovej techniky, informačných systémov, služieb alebo IKT infraštruktúry v správe CVT.

Cieľom helpdesku je poskytovať rýchlu a efektívnu pomoc používateľom, a súčasne centrálne spravovať a dokumentovať požiadavky a ich riešenia.

Požiadavky alebo problémy sa zaznamenávajú ako tikety, ktoré obsahujú relevantné podrobnosti, ako opis problému, úroveň priority a aktuálny stav riešenia. Tiket v sebe obsahuje vlákno správ medzi koncovým používateľom a špecialistom technickej podpory.

Helpdesk je dostupný ako webová aplikácia na adrese https://helpdesk.stuba.sk, cez ktorú môžete zadať novú požiadavku (tiket) aj bez prihlásenia sa.

Druhý spôsob práce s helpdeskom je jednoduché odoslanie e-mailu s požiadavkou na adresu helpdesk@stuba.sk, čo rovnako vytvorí tiket a používateľské konto, ak ešte neexistuje.

Manuál k Helpdesku nájdete na web stránke:
https://www.stuba.sk/sk/pracoviska/centrum-vypoctovej-techniky/navody/helpdesk-stu-pouzivatelsky-manual.html?page_id=16454

V Bratislave dňa : 09.06.2025

Ing. Marian Ďurkovič
riaditeľ CVT STU