VÝNOS KVESTORA Č. 4/2021
UŽÍVÁNÍ A SPRÁVA IT NA AVU

zpracovatel a věcně odpovědná osoba:	Tomáš Kuchař, vedoucí ITO ve spolupráci Tomáš Kukla, bezpečnostní expert Balcom
schválil:	PhDr. Evžen Mrázek, kvestor
schváleno dne:	31.8.2021
nabývá účinnosti ode dne:	1.9.2021
kontrola aktuálnosti výnosu:	každoročně

ČLÁNEK 1

Vymezení pojmů

1.1 Výnos je platný pro Akademii výtvarných umění v Praze (dále jen „AVU“ nebo „akademie“).

1.2 Pojem IT – Informační technologie – se pro účely tohoto výnosu rozumí veškeré hardwarové, softwarové a další technické prostředky výpočetní a telekomunikační techniky používané jak v AVU, tak i na prostředky používané mimo prostory akademie v případě, že je AVU jejich vlastníkem.

1.3 Počítačová síť AVU (dále jen „počítačová síť“) zahrnuje veškeré počítače, servery a mobilní zařízení připojené do počítačové sítě AVU, instalovaný software na těchto počítačích, serverech a mobilních zařízeních a veškeré technické zařízení zajišťující provoz počítačové sítě.

1.4 IT zařízení je osobní počítač (PC), notebook či obdobné zařízení (např. mobilní telefon, tablet apod.), využívané pro běžnou práci uživatelů apod. Výnos se vztahuje i na počítače nepřipojené k počítačové síti AVU, pokud jsou evidovány v majetku AVU.

1.5 Server je počítač vyhrazený pro poskytování síťových služeb ostatním počítačům a uživatelům počítačové sítě AVU.

1.6 Technické zařízení zajišťující provoz počítačové sítě jsou zařízení a prostředky umožňující propojit počítače, servery a připojit celou počítačovou síť k internetu (aktivní prvky, kabelové rozvody, zásuvky apod.)

1.7 Uživatel/ka je každá osoba, která používá některý z prostředků a zařízení IT AVU.

1.8 Správce je osoba pověřená správou některého z prostředků informačních technologií AVU.

1.9 Ohlašovatel/ka je osoba, která zpracovává požadavky na správu počítačové sítě od uživatelů a předává požadavky správcům počítačové sítě. Tato osoba je mimo vedení AVU jediná oprávněná zadávat požadavky správcům počítačové sítě. Ohlašovatele určuje vedení AVU.

1.10 Kontakt na ohlašovatele je: https://helpdesk.avu.cz. V případě osobního nahlášení zaměstnancům IT oddělení nebo externím správci sítě AVU, platí povinnost ex post nahlásit událost prostřednictvím https://helpdesk.avu.cz. Administrátory je přípustné ve výjimečných situacích kontaktovat telefonem i osobně.

1.11 Serverovna je technická místnost, kde se nachází centrální zařízení počítačové sítě (server, switche apod.).

ČLÁNEK 2

Správci

2.1 Správci IT jsou: zaměstnanci IT oddělení a zaměstnanci externího správce sítě. Seznam, odpovědnosti a kontakty na správce IT jsou uvedeny v aplikaci HELPDESK na adrese https://helpdesk.avu.cz.

2.2 Správce IT je zodpovědný za IT AVU jako celek. Navrhuje a podílí se na realizaci rozvoje IT v souladu se záměry a ve spolupráci s vedením AVU. Řídí a kontroluje činnost všech ostatních správců jednotlivých prostředků IT. Vedoucí IT oddělení řídí a kontroluje externího správce IT. Správce IT je zodpovědný za bezproblémový chod celé počítačové sítě.

2.3 Správce uživatelů je osoba pověřená vedením evidence uživatelů, přidělováním uživatelských jmen a hesel, správou přístupových systémů a systémů elektronického zabezpečení.

2.4 **Uživatelé počítačové sítě nesmí předávat žádné informace o počítačové síti nebo povolit přístup k jakékoli části počítačové sítě ostatním osobám, pokud to správce IT předem neschválil**.

ČLÁNEK 3

Odpovědnost a pravomoci správců

3.1 Uživatelé počítačové sítě jsou povinni respektovat pokyny a doporučení vydané příslušnými správci, pokud jsou v souladu s touto směrnicí nebo jsou objektivně odůvodnitelné vzhledem k okamžitému stavu IT s ohledem na zajištění bezproblémového chodu a bezpečnosti IT.

3.2 AVU v případě potřeby zajistí správci přístup ke všem částem počítačové sítě.

ČLÁNEK 4

Pravidla používání počítačové sítě a prostředků IT

4.1 Každý uživatel počítačové sítě je povinen seznámit se s aktuálním zněním tohoto výnosu a dodržovat ho.

4.2 Každý uživatel písemně potvrdí, že zná a bude dodržovat tento výnos.

4.3 Uživatel nesmí vyvíjet takovou činnost, která by poškozovala IT AVU nebo která by ostatním uživatelům škodila nebo bránila v řádném využívání IT AVU.

4.4 Porušení jakéhokoli bodu tohoto výnosu je možno postihnout.

4.5 AVU má možnost monitorovat činnost uživatelů v IT, zejména prováděním kontrol oprávnění a jejich přístupu ke službám, prostředkům a aplikacím v systému, využívání internetu, pokusům o neoprávněný přístup, instalaci a používání neodsouhlaseného SW a HW, využívaní poskytovaných služeb, provádění nepovolené činnosti apod.

4.6 **Uživatel je povinen:**

- užívat přidělené zařízení a prostředky IT pouze v rozsahu nutném pro plnění pracovních povinností a svěřených úkolů a jen v rozsahu přidělených přístupových práv;
- pracovat s prostředky a zařízením tak, aby je nepoškodil, zejména mechanicky;
- přihlašovat se pro práci do IT vždy jen pod svým uživatelským účtem (s výjimkou testování vyvíjených produktů, kdy je vyžadováno přihlášení k vyvíjené aplikaci pod jinou identitou);
- zpracovávat informace pouze v souladu s přidělenými uživatelskými přístupovými právy;
- chránit na používaném IT zařízení zpracovávané informace v souladu s článkem 9. Zabezpečení, hesla, kódy, přístupový systém;
- pořizovat nebo modifikovat data v IT pouze v souladu se skutečností a v rozsahu svého oprávnění;
- důsledně dodržovat pravidla antivirové prevence, kontrolovat všechny přijaté soubory na přítomnost virů, a to včetně souborů na výměnných médiích, stažených z internetu nebo připojených k e-mailu před jejich použitím, otevřením nebo zkopírováním do IT;
- při každém opuštění svého pracoviště (i dočasném) zajistit, aby žádná osoba nemohla na IT zařízení pracovat bez řádného přihlášení (dodržovat „pravidlo čisté obrazovky“) - například okamžitým spuštěním spořiče obrazovky, který je chráněn heslem, uzamknutím IT zařízení (Ctrl-Alt-Del s následným výběrem volby „Uzamknout počítač“ u PC s OS Windows 2000 a vyšších nebo Windows klávesa + L), standardním ukončením práce s IT zařízením nebo jeho vypnutí apod.;
- zachovávat mlčenlivost o obsahu, možnostech zpracování a způsobu zajištění bezpečnosti chráněných informací vyskytujících se v IT;
- počínat si tak, aby chráněná data a informace nemohly být odposlechnuty, odpozorovány, nebo vyčteny ze zpracovávaných dokumentů a obrazovek neoprávněnými osobami;
- ukládat data do stanovených složek, adresářů a aplikací;
- zálohovat data zpracovávána v IT na přenosné nosiče informací pouze předepsaným způsobem;
- přenosná média určená k likvidaci předávat vždy k likvidaci pouze bezpečnostnímu správci IT;
- nahlásit zjištění každého bezpečnostního incidentu nebo slabiny v IT bez zbytečného prodlení správci IT;
- dodržovat licenční politiku používaného SW a respektovat autorskoprávní ochranu dat;
- provádět tvorbu a změny hesel podle stanovených podmínek v čl. 9;
- uchovávat veškeré převzaté doklady k nainstalovanému SW a HW;
- důsledně zálohovat, popřípadě archivovat, veškerá data, pokud nejsou uložena na centrálních zálohovaných prostředcích;

- neprodleně poskytovat potřebnou součinnost správcům IT v případě plánované údržby IT zařízení, při poruchách, závadách, při podezření na oslabení zabezpečení nebo při jiných obdobných činnostech.

ČLÁNEK 5

Pravidla používání IT zařízení

5.1 Za dodržování pravidel při práci na IT zařízení zodpovídá uživatel, kterému je zařízení přiděleno.

5.2 Uživatel nesmí bez souhlasu správce zasahovat do hardwarové konfigurace IT zařízení. Případné problémy s hardwarem uživatel řeší se správcem.

5.3 Uživatel nesmí instalovat žádný software na IT zařízení. Pokud toto pravidlo poruší, odpovídá za případné škody způsobené instalací.

5.4 Za každé nové IT zařízení, které uživatel obdrží, musí uživatel podepsat předávací protokol.

5.5 Každý počítač nebo zařízení musí být chráněné heslem a uživatel tuto ochranu nesmí rušit nebo oslabovat.

5.6 Uživatel nesmí mít k dispozici administrátorské oprávnění k IT zařízení. V případě že takové oprávnění požaduje, může mu být po určitou dobu uděleno na základě schválení žádosti kvestorem AVU. V případě, že takové oprávnění má k dispozici bez žádosti, musí tuto skutečnost oznámit vedoucímu IT oddělení.

5.7 Při odchodu z místnosti, kde je umístěno IT zařízení, musí uživatel zařízení uzamknout (například kombinace kláves: Windows + L) a u pevného počítače dále vypnout monitor.

5.8 Při delší nečinnosti uživatele se počítač automaticky uzamkne. Doba automatického uzamknutí počítače nesmí přesáhnout 15 minut.

5.9 Každý uživatel zodpovídá za to, že při opuštění IT zařízení nebudou zobrazeny důvěrné informace nebo osobní informace.

5.10 Zaměstnanec nesmí bezdůvodně nechávat zapojený napájecí zdroj v síti.

5.11 Je přísně zakázáno:

a) zobrazovat důvěrné informace neoprávněné třetí osobě
b) spouštět nepovolený nebo nelegální SW
c) spouštět programy špehující počítačovou síť
d) spouštět programy na prolamování hesel
e) provádět instalace nebo aktualizace prostřednictvím jiných osob, než jsou správci IT

5.12 V případě odcizení nebo ztráty IT zařízení AVU musí uživatel tuto skutečnost bez prodlení nahlásit správci.

ČLÁNEK 6

Mobilní IT zařízení

6.1 Každé mobilní IT zařízení musí mít nastaveno šifrování úložiště dat (pevný disk, flash disk aj.). Uživatel takové šifrování nesmí rušit nebo oslabovat.

6.2 Mobilní IT zařízení nesmí uživatel nechávat na nezabezpečeném nebo nevhodném místě bez dozoru (např. automobil, kavárna, v přítomnosti nepovolané osoby apod.).

ČLÁNEK 7

Tiskárny

7.1 Doplňování papíru zajišťuje uživatel tiskárny.

7.2 Výměnu toneru zajišťuje uživatel tiskárny, v případě pronajatých tiskáren osoba pověřená pronajímatelem tiskáren.

7.3 Uživatelé nesmí konfigurovat tiskárnu, bez předchozího schválení správcem IT.

7.4 Tisknout může uživatel pouze nezbytné materiály, které souvisejí s pracovní náplní.

7.5 Uživatelé nesmí nechávat vytisknuté materiály bez dozoru, musí zajistit ochranu osobních údajů.

ČLÁNEK 8

Uživatelské účty a oprávnění

8.1 Zřizování, rušení a změna uživatelských účtů a příslušných oprávnění (dále jen „změna účtu a oprávnění uživatele“) v počítačové síti je v kompetenci správce IT.

8.2 Správce IT změní účet a oprávnění uživatele na základě žádosti.

8.3 Žádost pro změnu účtu a oprávnění uživatele zadává nadřízený uživatele na základě žádosti v HelpDesku s dostatečným předstihem. Úprava účtu musí být dále schválena vedoucím pracovníkem IT.

8.4 Změnu účtu nebo oprávnění uživatele zaeviduje správce IT do „Evidence oprávnění“.

ČLÁNEK 9

Zabezpečení, hesla, kódy, přístupový systém

9.1 Uživatelé mají přesně vymezená oprávnění a rozsah přístupu do každého informačního systému (včetně souborového systému), k aplikacím, síťovým diskům a databázím.

9.2 Přístupy do informačních systémů jsou zabezpečeny unikátními uživatelskými jmény s přístupovými hesly (dále jen „přístupové informace“)

9.3 Požadavky na přístupová hesla jsou následující:

a) Požadavky na složitost hesla jsou minimálně 10 znaků, alespoň jedno malé a velké písmeno, číslice a speciální znak.
b) Změna hesla by měla být provedena nejpozději jednou za 180 dnů.
c) Unikátnost hesla (počet změn po sobě) je 10 změn.
d) Po 5 neúspěšných pokusech o přihlášení dojde k zablokování účtu.
e) Systém bude vynucovat dodržování požadavků na změnu hesla v nejzazším termínu.
f) Je zakázáno zapisovat si přístupová hesla a kódy v jakékoliv podobě. Přípustné je pouze ukládání přístupových údajů ve správci hesel. Správce hesel musí využívat šifrování AES s 512 bitovým klíčem. Dále musí podporovat automatické uzavření po krátké době. Hlavní heslo do manažera musí obsahovat více než 24 znaků.

9.3 Správce IT sděluje uživatelům přístupové informace písemnou formou tak, aby nemohlo dojít k jejich zneužití.

9.4 Při prvním přihlášení po přidělení hesla správcem IT je nutné heslo změnit tak, aby jej znal pouze uživatel.

9.5 Uživatelé jsou povinni udržovat své přístupové informace v tajnosti, aby nemohlo dojít k jejich zneužití. Za zneužití svých přístupových informací plně odpovídá uživatel, nebo ten, kdo uživateli tuto přístupovou informaci poskytl.

9.7 Správce IT dále přiděluje oprávněným osobám kódy k přístupovému systému a systému elektronického zabezpečení. Uživatel s těmito kódy nakládá stejně jako s hesly počítačové sítě a odpovídá za to, aby nemohly být zneužity.

9.8 Správce IT je zodpovědný za včasné zrušení přístupových hesel a kódů pro osoby, které přestali být uživateli prostředků IT AVU a změnu případných hromadných hesel a kódů. Skutečnost, že osoba již není uživatelem, musí být správci IT sdělena včas za pomocí formuláře.

9.9 Je přísně zakázáno vstupovat do informačních systémů a na síťová úložiště, do kterých nebyly získané přístupové údaje v souladu s platnými předpisy.

9.10 Je přísně zakázáno zkoušet prolomit jakoukoliv ochranu IS nebo zařízení.

ČLÁNEK 10

Údržba prostředků IT, odstávky

10.1 Pokud některá z těchto činností vyžaduje dlouhodobější odstávku síťové služby či serveru, jsou o tom uživatelé bezodkladně informováni (mail apod.). Takovéto činnosti by měli být prováděny v době malého vytížení služeb a serverů, pokud to situace dovolí.

10.2 Operativní a bezpodmínečně nutné či akutní zásahy mohou správci provádět i bez předchozího upozornění uživatelů. Musí se snažit minimalizovat dobu nepřístupnosti služby a dopad na uživatele. To nezbavuje povinnosti správce IT bezodkladně informovat vedení AVU dohodnutým způsobem.

10.3 Bezpečnost a spolehlivost provozu má přednost před komfortem uživatelů.

ČLÁNEK 11

Pořizování HW a SW, řešení problémů s HW, opravy

11.1 Pořizování nového hardwaru a softwaru spadá do kompetence vedení AVU.

11.2 Uživatelé předávají své požadavky prostřednictvím HelpDesk. Správce IT zajišťuje nabídku na vhodnou variantu nákupu.

11.3 Návrh je po schválení vedením AVU předán k vlastní realizaci nákupu.

11.4 Při problémech s funkčností HW je třeba se obrátit na příslušného správce IT, bez jeho vědomí se nesmí uživatel sám pokoušet závadu odstraňovat. Správce IT rozhodne o dalším postupu – nákup nového hardware, zajištění opravy. Pokud je to možné, zajistí neprodleně (alespoň dočasnou) náhradu za nefunkční hardware.

ČLÁNEK 12

Připojování zařízení do počítačové sítě AVU

12.1 Do počítačové sítě lze připojit pouze správcem IT povolené počítače a obdobná zařízení.

12.2 Připojení se týká jak pevného připojení, tak bezdrátového připojení.

ČLÁNEK 13

Datová úložiště

13.1 Datové úložiště na serverech je chráněno před přístupem ostatních uživatelů a jeho využití je plně v kompetenci uživatele.

13.2 Na serveru mohou být zřízena i sdílená datová úložiště přístupná definované skupině uživatelů a sloužící k výměně dat mezi těmito uživateli.

13.3 Na datová úložiště je přísně zakázáno ukládat nelegální obsah.

13.4 Datová úložiště slouží výhradně pro pracovní účely.

13.5 Nové složky na datovém úložišti smí vytvářet pouze správce IT, ostatní složky budou nenávratně odstraněny.

13.6 Důvěrné informace mohou být uloženy pouze v soukromých složkách, za tyto informace odpovídá uživatel.

ČLÁNEK 14

Citlivé informace AVU a osobní údaje

14.1 Citlivé informace AVU jsou všechny informace, které v případě neoprávněného použití mohou poškodit AVU, studující nebo její zaměstnance či zaměstnankyně.

14.2 Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

14.3 Je přísně zakázáno poskytovat citlivá data neoprávněným osobám.

14.4 Přenos citlivých dat je nutný dostatečně zabezpečit pomocí šifrování pomocí bezpečného hesla nebo certifikátu. Heslo pro dešifrování musí být přenášeno jiným komunikačním kanálem (osobně, sms apod.).

ČLÁNEK 15

Používání a manipulace s přenosnými datovými nosiči

15.1 Přenosný datový nosič, je jakékoliv médium, které slouží pro uchovávání a přenos informací (CD, USB Flash disk atp.) – dále jen „datové nosiče".

15.2 Používání datových nosičů je dovoleno pouze v případě, že nelze využít jiný způsob přenosu dat (například síťové úložiště).

15.3 Data AVU nesmí být vynášena z prostor AVU bez souhlasu vedení. Vedení musí být informováno o skutečné povaze těchto dat.

15.4 Data AVU mohou být uložena na datovém nosiči pouze po dobu nezbytně nutnou. Následně musí být data vymazány. I po běžném vymazání je možné data obnovit, proto před likvidací datového nosiče nebo změně užití je nutné provést trvalé odstranění dat, které provede na požádání správce IT.

15.5 Datové nosiče s citlivými daty musí být dostatečně zabezpečeny pomocí šifrování (například pomocí technologie Bitclocker nebo VeraCrypt).

ČLÁNEK 16

Serverovna

16.1 Do serverovny může přistupovat pouze vedení AVU a správce IT.

16.2 Uživatelé nebo jiné osoby (technik, úklid, správce budovy apod.) nesmí bez předchozího souhlasu správce IT nebo vedení vstupovat do serverovny. Je-li mu udělen souhlas o přístupu, musí před přístupem zapsat důvod a čas, kdy vstupuje do serverovny na přístupovou listinu a potvrdit vlastnoručním podpisem. Ohlašovatel, správce IT nebo vedení AVU doplní po opuštění uživatele nebo osob ze serverovny čas odchodu.

16.3 Serverovna nesmí sloužit ke skladování materiálu nebo odpadu, který nesouvisí s prvky počítačové sítě.

16.4 Při každém odchodu ze serverovny musí uživatelé nebo jiné osoby serverovnu ihned zabezpečit. Správce IT musí serverovnu zabezpečit pokaždé, když ukončí činnost na AVU.

ČLÁNEK 17

Email

17.1 Zaměstnanec má vytvořenou emailovou schránku s příslušnou emailovou adresou nebo adresami, pokud to vedení uzná za vhodné.

17.2 Tato mailová adresa je považována za jeden z oficiálních kontaktů daného uživatele.

17.3 Emailová adresa je určena pouze pro komunikaci, která souvisí s pracovní náplní uživatele.

17.4 V žádném případě nesmí být používána pro komerční rozesílání emailových zpráv třetích stran, které nesouvisí s pracovní nebo školní náplní uživatele.

17.5 Poštovní server může být vybaven antispamovým a antivirovým softwarem. Tuto ochranu však nelze považovat za stoprocentní, a proto je třeba chovat se zodpovědně i na straně uživatele (antivirový software, filtrace spamu u uživatele, obezřetné zobrazování emailových zpráv).

17.6 Vědomé rozesílání spamu z emailové adresy uživatele nebo jiné zneužití emailové schránky je zakázáno.

ČLÁNEK 18

Viry, antivirový software

18.1 Na IT zařízeních jsou nainstalované antivirové programy.

18.2 Uživatel pracující na takovém počítači nesmí antivirovou ochranu vypínat nebo oslabovat.

ČLÁNEK 19

Závěrečná ustanovení

19.1 Tento výnos schvaluje kvestor po projednání s vedením AVU.

19.2 Každý uživatel smí k tomuto výnosu vznášet připomínky a návrhy na doplnění a úpravy.

19.3 Rozhodnutí o skutečnostech výslovně neuvedených v tomto výnosu je plně v kompetenci vedení AVU nebo správce IT, který o rozhodnutí neprodleně informuje vedení AVU.

19.4 Tento výnos vstupuje v platnost dnem zveřejnění a platí až do odvolání nebo zveřejnění nové verze tohoto výnosu.

19.5 O případném zveřejnění nové verze výnosu jsou uživatelé včas informováni.

ČLÁNEK 20

Ochrana dat a informací

AVU chrání občanská, osobní i vlastnická práva všech uživatelů IT a v této souvislosti chrání i data a informace uložená nebo přenášená IT.

AVU nemůže zajistit úplnou bezpečnost chráněných informací v IT pouze technickými prostředky, proto je k jejich ochraně použita celá řada dodatečných prostředků.

Osobní údaje

Ochrana osobních údajů je v AVU zajišťována v souladu s Obecným nařízením o ochraně osobních údajů. Způsob zajišťování ochrany této kategorie informací je obsažen v dokumentu „Výnos rektora č. 5/2020 - ochrana a zpracování osobních údajů“.

Pro zajištění maximální možné míry soukromí a bezpečnosti dat je uživatelům dále zakázáno:

- provádět jakékoli akce, které vedou k narušení soukromí jiného uživatele, a to i v případech, kdy uživatel svá vlastní data explicitně nechrání;
- kopírovat jakákoliv data nebo programy z uživatelských adresářů (home adresáře) bez souhlasu jejich majitele (to zahrnuje i samotné prohlížení těchto adresářů); toto omezení se nevztahuje na sdílené složky a adresáře;
- používat síť k získání neautorizovaného přístupu k neveřejným informačním zdrojům (i v majetku/správě jiných organizací).

Článek 21

Výnos kvestora k užívání a správě IT je součástí systému dalších dokumentů k pořizování, ochraně a správě informací pořizovaných a spravovaných AVU za účelem naplnění jejího poslání. Mezi nejdůležitější dokumenty patří

- Výnos rektora AVU ke kybernetické bezpečnosti
- Systém řízení bezpečnosti informací AVU
- Výnos kvestora ke kamerovému systému
- A další