Pravidla užívání internetu a jeho bezpečnost

Základní pravidla užívání sítě Cesnet (síť AV ČR je její součástí) jsou obsažena v *Zásadách přijatelného užití infrastruktury* (Acceptable Use Policy, AUP)

1. Účastník je oprávněn užívat Infrastrukturu pro aktivity, které jsou v souladu s těmito Zásadami přijatelného užití Infrastruktury, s dobrými mravy, respektují potřeby ostatních účastníků a šetří zdroje Infrastruktury. Účastník je povinen při užívání Infrastruktury dodržovat zákony a další právní předpisy, které jsou součástí právního řádu České republiky. Tímto ustanovením není dotčeno právo Sdružení na případnou náhradu způsobené škody ani občanskoprávní nebo trestněprávní odpovědnost účastníků Infrastruktury.
2. Účastník nesmí používat Infrastrukturu zejména pro činnosti, které:
    2.1. mají povahu neoprávněného užití, zásahu, změny počítačových systémů, jejich částí, nosiče informací nebo dat;
    2.2. porušují práva duševního vlastnictví;
    2.3. nepříznivě působí na provoz Infrastruktury nebo jejích jednotlivých služeb, brání dalším účastníkům v přístupu k těmto službám, ohrožují řádný provoz Infrastruktury nebo nadměrně omezují její 3.výkon.
3. Pro užívání Infrastruktury jinými subjekty musí účastník požádat předem o souhlas Sdružení.
4. Účastník je povinen zajistit, aby ze zařízení v jeho působnosti (jím vlastněných, najatých, vypůjčených, provozovaných apod.) nebyla Infrastruktura využívána k účelům odporujícím těmto Podmínkám či smlouvě, na základě které účastník využívá služby Infrastruktury.
5. Pokud Účastník užije Infrastrukturu nebo informace o ní v rozporu s těmito Zásadami přijatelného užití Infrastruktury nebo smlouvou, na základě které účastník získal přístup k Infrastruktuře, nebo k takovému užití napomůže třetí osobě úmyslně nebo zanedbáním, je povinen uhradit Sdružení náhradu vzniklé škody.
6. Podmínky využití jednotlivých služeb Infrastruktury jsou dostupné na internetových stránkách Sdružení www.cesnet.cz/sluzby.

Jako příklad pravidel užívání lokálních sítí pracovišť AV ČR lze použít výtah z Pravidel užívání počítačů a počítačové sítě utia.cas.cz

Povinnosti a práva uživatelů počítačových prostředků

a) Každý nový uživatel před započetím práce s počítačovými prostředky písemě potvrdí, že zná tato "Závazná pravidla" a bude je dodržovat.
b) Uživatel smí používat počítačové prostředky pouze v rámci své pracovní náplně a v souladu s výzkumným a vzdělávacím posláním Akademie věd ČR. Je zakázáno přenášet počítačovou sítí soubory, jejichž obsah je v rozporu se zákonem. Dále je zakázáno používat počítačovou síť ke komerčním účelům (inzerce, školení, poskytování informací, programů a dat ze sítě za úplatu

apod.). Výjimku může písemně povolit pro počítačovou síť Ústavu správa sítě Ústavu nebo vedení Ústavu.

c) Uživatel pracuje na počítačových prostředcích pouze pod tím uživatelským jménem, které mu bylo přiděleno. Heslo ke svému uživatelskému jménu volí a udržuje v tajnosti tak, aby bylo zabráněno jakékoliv možnosti zneužití; při volbě hesla je povinen respektovat doporučení správy sítě. Uživatel zodpovídá za škody, vzniklé v důsledku zneužití jeho uživatelského účtu, které bylo umožněno nedbalým zacházením s heslem.
d) Přístupová práva uživatele jsou dána jeho uživatelským jménem a účastí ve skupinách uživatelů. Uživatel se nesmí žádným způsobem pokusit získat přístupová práva nebo privilegovaný stav, který mu nebyl přidělen administrátorem sítě. Jestliže uživatel získá uživatelská práva nebo privilegovaný stav, které mu nepatří, a to jakýmkoliv způsobem včetně hardwarové nebo softwarové chyby počítačových prostředků, je povinen tuto skutečnost neprodleně oznámit administrátorovi sítě.
e) Uživateli je zakázáno vědomě používat a šířit nelegální software a počítačové viry. Uživateli není dovoleno pokusit se získat přístup ke chráněným informacím, programům a datům jiných uživatelů. Rovněž je zakázáno kopírovat a distribuovat části operačního systému a instalovaných programů a souborů, pokud to držitel autorských práv k těmto programům a souborům výslovně nepovolil.
f) Uživatel nesmí vědomě narušovat práci ostatních uživatelů počítačové sítě ani chod a výkonnost sítě jako celku např. nadměrným zatěžováním zdrojů sítě. Při přístupu ke službám ve vnějších sítích je uživatel povinen využívat nejbližší servery sítě, které zadanou službu poskytují, a pokud možno mimo hlavní pracovní dobu lokálních uživatelů těchto serverů.
g) Pro používání elektronické pošty (E-mailu) platí stejná etická pravidla jako pro obyčejnou poštu, přičemž poštovní zpráva má charakter otevřené listovní zásilky. Je zakázáno používat E-mail pro šíření obchodních informací nebo pro politickou či náboženskou agitaci. Uživatel je povinen dbát na to, aby jeho zprávy byly přesně adresované a nedocházelo k obtěžování ostatních uživatelů.
h) Uživatel nesmí svévolně měnit konfiguraci počítače nebo terminálu připojeného do počítačové sítě Ústavu způsobem, který by mohl ovlivnit provoz sítě. Takové změny v konfiguraci je třeba předem projednat s administrátorem sítě.

Povinnosti a práva správy sítě

a) Správa počítačové sítě a její administrátoři jsou povinni dbát na to, aby počítačové prostředky Ústavu byly využívány v souladu s těmito "Závaznými pravidly".
b) Fyzické připojení a odpojení zařízení k počítačové síti Ústavu a změny architektury a topologie sítě provádějí pouze pracovníci správy sítě na základě svého rozhodnutí. Výjimky povoluje správa sítě.
c) O možnosti připojení dalších prostředků výpočetní techniky do počítačové sítě rozhoduje správa sítě.
d) V případě poruchy na síti má administrátor sítě právo odpojit segment sítě, který způsobuje problémy, na nezbytně nutnou dobu, aby byla zachována funkčnost sítě Ústavu. O příčinách a postupu odstraňování závad správa sítě informuje příslušný okruh uživatelů.

Postihy za nedodržení těchto pravidel

a) Nedodržení těchto "Závazných pravidel" zaměstnancem Ústavu bude považováno za porušení základních povinností pracovnika podle §73, odst. 1, písmene b), c) a d) Zákoníku práce. Porušování těchto povinností je porušením pracovní kázně a vedení Ústavu může uplatnit vůči provinilým pracovníkům postih v souladu se Zákoníkem práce.
b) Nedodržení těchto "Závazných pravidel" osobami, které nejsou zaměstnanci Ústavu, může být postihnuto odnětím práva přístupu k počítačovým prostředkům Ústavu bez náhrady.
c) Hrubé porušení "Závazných pravidel" může být rovněž předmětem soudního stíhání podle občanského nebo trestního práva.

10 doporučení pro bezpečné chování na internetu

1. Volte hesla bezpečná, nikoliv jednoduše zapamatovatelná
2. Zajímejte se o to, komu svěříte své osobní údaje. Vždy si dobře rozmyslete, komu poskytnete své osobní údaje. Velmi problematické také bývá vyplnění platebních údajů. Ty zadávejte pouze v rámci ověřeného internetového bankovnictví, případně v důvěryhodných platebních branách. Nepoužívejte internetové bankovnictví z veřejných míst na Wi-Fi.
3. Platťte obezřetně, zadávejte své osobní údaje jen při připojení, které je ověřené, bezpečné a šifrované („https“ místo klasického http“)
4. Nestahujte neověřený obsah
5. Používejte aktualizovaný antivirový program
6. Mějte dvě e-mailové adresy: jednu pro osobní účely, druhou pro registrace do internetových služeb
7. Ujistěte se, že v rámci sociálních sítí a dalších internetových služeb poskytujete jen minimální množství osobních informací a že citlivé údaje vaší osoby nejsou viditelné všem.
8. Buďte obezřetní při práci na veřejných nezabezpečených sítích vyhněte se zadávání citlivých osobních údajů.
9. Vyhýbejte se potenciálně podezřelým webovým stránkám
10. Nepřidávejte si na sociálních sítích neznámé kontakty, a to ani v okamžiku, kdy má protějšek s vámi několik společných přátel a je velmi atraktivní. A v neposlední řadě nikomu cizímu, ale ani vašim přátelům, jejichž účet mohl být ukraden, neposkytujte vaše telefonní číslo, citlivé údaje nebo kódy, které vám v rámci SMS přijdou.

OBECNÁ PRAVIDLA BEZPEČNĚJŠÍHO CHOVÁNÍ NA INTERNETU

JAK (NE)KOMUNIKOVAT?

1. Nevěřte všemu, co se na internetu dozvíte. Informace ověřujte z více zdrojů.

2. Nezveřejňujte o sobě na internetu žádné citlivé informace.

3. Nikomu neposílejte své intimní fotografie. Ani je veřejně nesdílejte.

4. Dávejte pozor na podezřelé zprávy, přílohy, videa a odkazy.

5. Ověřte si totožnost člověka, se kterým komunikujete

CO (NE)DĚLAT PO TECHNICKÉ STRÁNCE?

1. Pro přístup do informačních systémů s citlivými informacemi vždy používejte vícefaktorovou autentizaci.

2. Nikomu nesdělujte své přihlašovací údaje. Pravidelně je aktualizujte. Používejte silná a unikátní hesla. (Silné heslo: minimálně 8 znaků, kombinace písmen, číslic a speciálních znaků.) (Unikátní heslo: použito pro přístup pouze k jednomu účtu nebo zařízení.)

3. Na veřejných počítačích (na univerzitě, v knihovně, v kavárně) nikdy nepřistupujte k důvěrným sítím nebo datům a neukládejte hesla a přihlašovací údaje do paměti prohlížeče.

4. Udržujte své antivirové zabezpečení aktualizované Své zařízení pravidelně testujte.

5. Zálohujte soubory ve svém zařízení na externí disky nebo do cloudu. V případě potřeby můžete svá data kdykoli obnovit.

6. Neotevírejte obsah nalezených paměťových zařízení na svém počítači.

7. Když používáte nezabezpečenou veřejnou WiFi síť, nikdy na ní nenakupujte, nekontrolujte své účty ani nepřistupujte k důvěrným sítím nebo datům