Základní umělecká škola, Jablunkov,

příspěvková organizace



home office

## Povinnosti zaměstnance

## při využívání výpočetní techniky a práci s dokumenty organizace

## v rámci výkonu pracovní činnosti z domova (home office)

1. Zaměstnanec je povinen **listinné dokumenty** (jednotlivé dokumenty a spisy) pracovní povahy, které bude potřebovat k výkonu práce z domova:
   1. přenášet ze svého pracoviště domů výhradně v uzavíratelném obalu (např. taška, osobní kufřík, uzavíratelná složka apod.), z důvodu zamezení ztráty jednotlivého dokumentu (např. jeho náhodným vypadnutím z neuzavíratelné složky atd.);
   2. při převozu dokumentů automobilem:
      1. nenechávat přepravované listiny ve vozidle bez osobního dozoru, a to z důvodu předejití jejich ztráty v případě odcizení zaparkovaného vozidla nebo odcizení věcí z něj;
      2. uložit listiny ve vozidle takovým způsobem, který znemožní náhled na jejich obsah nepovolaným osobám (např. volně neodkládat dokumenty za čelní/zadní sklo nebo na sedadla);
   3. v místě bydliště listiny ukládat výhradně způsobem, který zamezí jejich nechtěnému přečtení, poškození, zničení nebo odcizení osobami, s nimiž zaměstnanec domácnost sdílí nebo které ho v ní navštěvují.
2. Při využití **výpočetní techniky organizace** k práci z domova, je zaměstnanec povinen:
   1. Mimo objekty organizace vykonávat pracovní úkoly pouze na zařízeních (notebooky) ve vlastnictví organizace.
   2. Pro práci a připojení k informačnímu systému organizace vždy využívat šifrovaného, zabezpečeného připojení pomocí VPN, či jiné obdobné, stejně bezpečné technologie, jejíž nastavení zabezpečuje správce ICT organizace.
   3. V případě připojení k informačnímu systému organizace prostřednictvím vzdálené plochy, po ukončení práce vždy uzavřít připojení vzdálené plochy.
   4. Neponechat zařízení bez dozoru v zapnutém stavu.
   5. Aktivně zabraňovat volnému odpozorování obrazovky cizí osobou, a to včetně rodinných příslušníků.
3. Soukromá zařízení (výpočetní techniku) smí zaměstnanec k výkonu práce z domova použít pouze na základě výslovného schválení ředitele organizace. V případě schválení musí zaměstnanec dodržovat tato pravidla:
   1. Soukromá zařízení, jejichž prostřednictvím zaměstnanec přistupuje k informačnímu systému organizace a aplikacím, musí být:
      1. Vybavena pravidelně aktualizovaným operačním systémem.
      2. Vybavena pravidelně aktualizovanou antivirovou aplikací.
      3. Chráněna za pomoci přihlašovacích údajů uživatele, s:
         * minimální délkou hesla: 8 znaků, a
         * použití alespoň 3 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky).
   2. Nastavena tak, aby se po 5 minutách neaktivity uživatele uzamknula.
4. Při používání výpočetní techniky organizace, včetně případně schválených soukromých zařízení, pro připojení k informačnímu systému organizace jsou zaměstnanci povinni:
   1. Učinit všechna dostupná opatření, která mohou zabránit ztrátě či odcizení zařízení (neponechávají je bez dohledu např. v autě, dopravních prostředcích, v ubytovacích zařízeních apod.).
   2. Pro připojení k internetu prostřednictvím Wi-Fi sítí využívat pouze šifrovaného, zabezpečeného připojení a po ukončení práce se neprodleně odpojit od této sítě (zásadně nevyužívat připojení prostřednictvím nezabezpečených „free“ Wi-Fi sítí).
   3. Aktivně zabraňovat odpozorování obrazovky cizí osobou (např. ve vlacích, restauracích, na lavičkách, v prostředcích hromadné dopravy apod.).
   4. Neumožnit přístup ke zpracovávaným informacím jiné osobě, včetně rodinných příslušníků.
5. Po ukončení práce z domova (po ukončení práce v režimu home office) zaměstnanec provede trvalé a neobnovitelné smazání veškerých pracovních dat ze soukromé výpočetní techniky (pokud tato byla k práci využita), vč. použitých paměťových médií. Zlikvidovány budou i kopie listinných dokumentů pořízených v souvislosti s výkonem pracovní činnosti pro zaměstnavatele.
6. V případě poškození, zničení, ztráty nebo odcizení listinného dokumentu, paměťového média, nebo výpočetní techniky (organizace nebo soukromé, na které byla ředitelem organizace povolena práce z domova) a dále v případě provedení kybernetického útoku na pracovní nebo soukromou výpočetní techniku užívanou k výkonu práce z domova, je zaměstnanec povinen tuto skutečnost neprodleně, po jejím zjištění, nahlásit svému přímému nadřízenému.

|  |  |  |  |
| --- | --- | --- | --- |
| P. č. | Jméno a Příjmení | datum | podpis |
|  | Ondřej Bazgier |  |  |
|  | Jan Drong |  |  |
|  | Ivana Funioková |  |  |
|  | Marek Kaleta |  |  |
|  | Marek Kaleta klavír |  |  |
|  | Katarzyna Kamińská |  |  |
|  | Karolína Kawuloková |  |  |
|  | Kateřina Kawuloková |  |  |
|  | Pavlína Kufová |  |  |
|  | Věra Miklerová |  |  |
|  | Kristina Mruzková |  |  |
|  | Ondřej Pazdera |  |  |
|  | Kristina Pyszková |  |  |
|  | Lucie Samiec |  |  |
|  | Tomáš Samiec |  |  |
|  | Jarmila Sikorová |  |  |
|  | Daniela Sławińska |  |  |
|  | Erika Sochacka |  |  |
|  | Petr Vondráček |  |  |
|  | Oldřich Volný |  |  |
|  | Dana Zońová |  |  |
|  | Martina Zońová |  |  |