

Klasifikace aktiv UTB

Označení		Veřejné	Interní	Chráněné
Zajištění důvěrnosti	Popis	Aktiva jsou již zveřejněné nebo byla určena ke zveřejnění (např. na základě zákona č.106/1999 Sb. o svobodném přístupu k informacím v platném znění), nepodléhají žádnému utajení. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy UTB. Tyto informace jsou považovány za Veřejné informace (zájemce o zaměstnání, uchazeč o studium).	Aktiva nejsou veřejně přístupná. Přístup k informacím je omezen na danou skupinu (zaměstnance a studenty UTB, dodavatele, partnery projektu, vývojáře služby, vybrané uživatele služby) a principem need-to-know, který stanovuje garant aktiva. Ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. Tyto informace jsou považovány za Komunitní informace.	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. strategické obchodní tajemství, zvláštní kategorie osobních údajů). Přístup k informacím je omezený garantem aktiva na okruh osob specifikovaných v rozdělovníku (seznam konkrétních osob, pracovních rolí nebo skupin osob), v případě elektronických systémů pak dle přiřazení ke konkrétní uživatelské skupině. Tyto informace jsou považovány za Chráněné informace.
	Požadovaná opatření	Není vyžadována žádná ochrana.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily a metody ochrany zabraňující kompromitaci ze strany administrátorů IT.
Zajištění integrity	Popis	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy UTB.	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů UTB a může se projevit méně závažnými dopady na primární aktiva.	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů UTB s přímými a velmi vážnými dopady.
	Požadovaná opatření	Není vyžadována žádná ochrana.	Pro ochranu integrity jsou využívány standardní nástroje např. omezení přístupových práv pro zápis.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu např. pomocí technologie digitálního podpisu.
Zajištění dostupnosti	Popis	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období nápravu (cca do 1 týdne).	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů UTB.	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů UTB. Aktiva jsou považována jako kritická.
	Požadovaná opatření	Pro ochranu dostupnosti je postačující pravidelné zálohování.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.