Příloha č. 4 - **Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele**

* Bezpečnost přístupových oprávnění
  + Poskytovatel je povinen chránit veškeré přístupové údaje k informačním aktivům objednatele včetně přístupů k informačním aktivům poskytovatele, které umožňují přístup k informačním aktivům objednatele či umožňují jejich správu.
  + Poskytovatel je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
    - min. délka hesla 17 znaků
    - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
      * malá písmena
      * velká písmena
      * číslice
      * speciální znaky
    - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě (dle bodu kryptografie)
    - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
    - platnost hesla musí být maximálně 1 rok.
  + Poskytovatel je povinen používat personifikované účty, které jsou nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
  + Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
  + Pokud by Poskytovatel zřizoval přístupová oprávnění třetí straně, je poskytovatel povinen o této skutečnosti informovat objednatele. Objednatel má v tomto případě právo zřízení přístupu zamítnout.
* Řízení kybernetických bezpečnostních incidentů:
  + Poskytovatel je povinen objednateli hlásit veškeré kybernetické bezpečnostní incidenty, které se týkají informačních aktiv objednatele nebo informačních aktiv poskytovatele, pokud se kybernetický bezpečnostní incident týká informací či informačních aktiv objednatele.
  + Poskytovatel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy objednatele.
* Řízení kontinuity činností
  + Poskytovatel se zavazuje plnit úkony definované v sestaveném a objednatelem odsouhlaseném disaster recovery plánu, který je součástí dodané provozní dokumentace.
* Řízení změn
  + Poskytovatel se zavazuje zaznamenávat všechny změny, které v informačním aktivu provedl.
  + Poskytovatel se zavazuje vynucovat zaznamenávání změn i u případných subdodavatelů.
  + Záznam změny musí obsahovat minimálně tyto informace:
    - Datum a čas změny
    - Jméno osoby, která změnu provedla
    - Název, popis a účel změny
  + Objednatel si vyhrazuje právo na pravidelné informace o záznamech všech změn provedených poskytovatelem i případnými subdodavateli.
  + Poskytovatel se zavazuje všechny jím provedené změny i změny případných subdodavatelů poskytnout objednateli formou pravidelného čtvrtletního reportu.