Audit IT ZČU

Datum:	
Společnost:	
Adresa:	

Obecné informace o společnosti (odpovědnost, systém řízení kvality)	**Popis**
Jaké standardy kvality jsou ve firmě používány (např. ISO 9001, ISO 15189….)?	
Kdo je pověřeným subjektem k certifikaci podle těchto norem? Prosím doložte dostupné certifikáty.	
Vyskytly se z těchto auditů nějaké závažné neshody?	
Kdo je zodpovědný za systém řízení kvality?	
Kdo je zodpovědný za zákaznický servis?	
Existuje organizační struktura a popis práce pro všechny pracovníky?	
Byl poskytovatel služeb ohrožen nežádoucími událostmi za posledních 5 let? Mezi tyto události patří únik dat, hacking, stížnosti na dodržování předpisů, pokuty, podvody a velké výpadky systému.	
Existuje systém pro interní audity systémů jakosti?	
Jak dlouho pracuje poskytovatel služeb ve svém oboru?	
Je servis poskytovaný FN Plzeň standardní servisní službou společnosti nebo jsou servisní služby upravované na míru?	
Technické dohody, zakázky	**Popis**
Existuje smlouva mezi společností a subdodavateli?	
Existuje systém pro příjem a potvrzení objednávek?	
Jak poskytovatel služeb zajišťuje soulad s platnými zákony a předpisy?	
Finance, stabilita	**Popis**
Potvrďte, že u poskytovatele služeb neexistují žádné významné aktuální závazky ani závazky, které by mohly ohrozit kontinuitu poskytovatele služeb.	

Bezpečnost, řízení rizik a dodržování předpisů	Popis
Jak je v organizaci poskytovatele služeb prováděno řízení bezpečnosti informací, řízení rizik a dodržování předpisů?	
Má poskytovatel služeb zavedený systém řízení kvality? Popište prosím.	
Jsou zpracovány SOP pro jednotlivé postupy?	
Jak je zabezpečeno, aby byla k dispozici aktuální verze všech dokumentů?	
Jaké jsou klíčové funkce a odpovědnosti za informační riziko, správu zabezpečení a dodržování předpisů?	
Jak jsou změny v systému řízení kvality dokumentovány a řízeny (postup, proces a materiály)?	
Má poskytovatel služeb systém pro zabezpečení informací, rizik a dodržování předpisů? Upřesněte prosím.	
Jak poskytovatel služeb hodnotí, sleduje a řeší rizika u subdodavatelů?	
Jak jsou navrženy procesy komunikace v případě vysoce rizikových incidentů?	
Poskytuje poskytovatel služeb prohlášení o ochraně osobních údajů a důvěrných informací podle GDPR? Upřesněte prosím.	
Má poskytovatel služeb nějaké osvědčení týkající se příslušných předpisů/zákonů o ochraně soukromí (např. směrnice EU o ochraně údajů)? Uveďte prosím certifikát a rozsah certifikace.	
Jak jsou vyšetřovány a řešeny stížnosti FN Plzeň na bezpečnost informací, rizika a dodržování předpisů poskytovatelem služeb?	
Má poskytovatel služeb zaveden formální proces validace týkající se služby dodávané FN Plzeň? Upřesněte prosím.	
Poskytuje společnost systémovou dokumentaci, kterou může FN Plzeň využít jako součást validačního procesu?	
Lidské zdroje	**Popis**
Má poskytovatel služeb zaměstnaneckou politiku? Upřesněte prosím.	
Má poskytovatel služeb specializovaný tým zaměstnanců, kteří budou pracovat na projektech pro FN Plzeň a budou mít přístup k jejím údajům? Upřesněte prosím.	

Je tým pracující pro systémy FN Plzeň kvalifikovaný a je řádně vyškolen k provozování služby? Upřesněte prosím.	
Jaký je proces prověřování zaměstnanců, kteří mají přístup k údajům FN Plzeň?	
Je poskytovatel služeb při poskytování služeb závislý na jedinečných zaměstnancích? Jak je poskytovatel služeb schopen vyrovnat se s jejich nepřítomností (např. nemoc, dovolená)?	
Logický přístup	**Popis**
Popište prosím ovládací prvky/mechanismy, které jsou implementovány, aby se zabránilo neoprávněnému použití systému a přístupu k datům.	
Je přístup k údajům FN Plzeň omezen pouze na oprávněný personál?	
Má poskytovatel služeb proces přidávání, změny nebo odvolání účtů a autorizací?	
Jsou uživatelské účty a autorizace opakovaně kontrolovány a znovu potvrzovány? Upřesněte prosím.	
Zabezpečení sítě	**Popis**
Jaká bezpečnostní opatření jsou přijata k ochraně sítě před neoprávněným přístupem? Například IDS/IPS, brány firewall, síťové zóny? Jak jsou provozovány?	
Jak je spravován vzdálený přístup k síti a případně služby poskytované FN Plzeň?	
Jaké jsou zásady pro nakládání s vyměnitelnými médii a jak je celý proces řízen?	
Jak zajišťujete konfiguraci síťové infrastruktury?	
Jak jsou kontrolovány a sledovány účty s oprávněními správce?	
Protokoly a monitorování	**Popis Logování a monitorování**
Má poskytovatel služeb zásady logování a monitorování? Upřesněte prosím.	
Jaké nástroje/mechanismy jsou implementovány pro monitorování bezpečnosti infrastruktury, aplikací a sítí? Upřesněte prosím.	
Jsou bezpečnostní protokoly pravidelně sledovány a kontrolovány? Upřesněte prosím.	

Může systém poskytovat přesné logy auditu pro zpracovaná data nebo jakýkoli typ transakcí? Upřesněte prosím.	
Jak jsou zabezpečeny uložené protokoly a kontrolní záznamy? Upřesněte prosím.	
Budou poskytnuty zprávy dokumentující spolehlivost systému? Můžete zaslat příklad takové zprávy?	
Anti Malware	**Popis**
Má poskytovatel služeb antimalwarové zásady? Upřesněte prosím.	
Jaký druh antimalwarového řešení je implementován?	
Jsou všechna příchozí a odchozí data testována na přítomnost malwaru? Upřesněte prosím.	
Jsou systémy a prostředky pro odhalování malwaru aktualizovány a jaký je interval?	
Správa oprav	**Popis**
Má poskytovatel služeb proces správy oprav?	
Jaké nástroje/mechanismy jsou implementovány k nepřetržitému/pravidelnému sledování hardwarové infrastruktury a aplikačního prostředí kvůli zranitelnostem?	
Probíhá na webových stránkách pravidelně kontrola zabezpečení webových aplikací? Upřesněte prosím.	
Objednává poskytovatel služeb v pravidelných intervalech nezávislý externí penetrační test? Upřesněte prosím.	
Jak je zajištěno, že nalezené chyby zabezpečení budou opraveny v akceptovatelném termínu?	
Správa změn a testů	**Popis**
Má poskytovatel služeb zdokumentovaný proces řízení změn? Upřesněte to.	
Jsou změny testovány a schváleny před jejich implementací?	
Jsou vývojová, testovací, akceptační a produkční prostředí oddělená?	
Je zajištěno, aby vývojoví pracovníci neměli práva zápisu do akceptačního a produkčního prostředí?	

Jak je zaručeno, že jsou testovány funkční a nefunkční požadavky?	
Je funkčnost systémů a procesů pravidelně vyhodnocována?	
Schvaluje oddělení kvality validační protokoly a zprávy?	
Jak jsou změny oznamovány zákazníkovi? Je možné, že zákazník změny odmítne (nebudou implementovány)? Upřesněte prosím.	
Data management	**Popis**
V jakém formátu jsou data zpracována nebo uložena? Prosím popište podrobněji.	
Po ukončení smlouvy: je technicky možné, aby poskytovatel služeb předal FN Plzeň data uložená poskytovatelem služeb v čitelném a upravitelném formátu?	
Po ukončení smlouvy: je technicky možné, aby poskytovatel služeb vymazal všechna data FN Plzeň, včetně zálohování?	
Má některý ze subdodavatelů poskytovatele služeb přístup k datům FN Plzeň? Jak je zajištěna důvěrnost, integrita a dostupnost v rámci subdodavatelů? Upřesněte prosím.	
Vyžaduje poskytovatel služeb připojení nebo rozhraní s externími stranami k poskytování služeb FN Plzeň? Jaké typy externích připojení se používají pro komunikaci s externími stranami?	
Má poskytovatel služeb zásady šifrování? Upřesněte prosím.	
Jak poskytovatel služeb spravuje šifrovací klíče?	
Jsou data při ukládání, zpracovávání a/nebo přenosu systémem šifrována? Upřesněte prosím.	
Je interní komunikace dat FN Plzeň zabezpečena šifrováním nebo hash funkcí? Upřesněte prosím.	
Pokud jsou zdroje sdíleny s ostatními zákazníky, jak poskytovatel služeb zajišťuje izolaci dat FN Plzeň od dat a služeb ostatních zákazníků?	

Fyzická bezpečnost	Popis
Je přístup do pracovního prostoru omezen pouze na oprávněný personál?	
Využívá poskytovatel služeb vlastní datové centrum? Nebo zapojuje poskytovatele datových center?	
Je datové centrum sdíleno s jinými subjekty? Pokud ano; jaká jsou opatření přijatá k zabránění neoprávněnému fyzickému přístupu do systémů?	
Je datové centrum certifikováno (ISO nebo ekvivalentně)? Poskytněte prosím platnou kopii certifikačního nebo účetního standardu.	
Kontinuita podnikání	**Popis**
Je součástí strategického plánu poskytovatele služeb plán kontinuity pro prostředí IT, klíčový personál a umístění podnikání?	
Je proces řízení kontinuity podnikání certifikován (např. ISO22301)?)?	
Jsou funkce/role, úkoly, odpovědnosti a pravomoci v rámci procesu řízení kontinuity podnikání oficiálně stanoveny a zdokumentovány?	
Jsou procesy, které jsou nezbytné pro dodávku produktů a služeb pro FN Plzeň, zahrnuty do rozsahu strategie a plánu kontinuity?	
Byla stanovena maximální tolerovatelná doba narušení procesů, které jsou zásadní pro dodávky (produktů a) služeb laboratoře HOO FN Plzeň? Jak je to zajištěno?	
Pro jakékoli subdodavatelské služby: jak poskytovatel služeb získá ujištění o kontinuitě služeb?	
Má poskytovatel služeb plán kontinuity činnosti a je tento plán pravidelně testován? Může poskytovatel služeb odeslat recenze nedávno provedených testů kontinuity provozu? Jak jsou výsledky testů vyřešeny a monitorovány?	
Máte plán komunikace, který by včas informoval všechny zúčastněné strany v případě krize?	

Proces řízení	Popis
Je výkon systémů poskytujících služby FN Plzeň jakýmkoli způsobem ovlivňován	
službami poskytovanými jiným zákazníkům? Upřesněte prosím.	
Jak poskytovatel služeb zajišťuje dohodnuté úrovně výkonu?	

Datum auditu: **Auditor:** **Podpis auditora:**