



TritonLife Magánkórházak Zrt.

INTEGRÁLT IRÁNYÍTÁSI POLITIKA

A TritonLife Magánkórházak Zrt. struktúrája, az ellátó egységek szakmai összetétele indokoltta teszi az integrált irányítási rendszer továbbfejlesztését, valamint az egységesen magas szintű ellátási minőség kiemelt szervezeti célként való kezelését.

Ennek érdekében a TritonLife Magánkórházak Zrt. vezetése **Minőségirányítási Egységes Rendszer koncepciót és stratégiát** határozott meg, fogadott el és ezúton nyilvánítja ki szándékát fenntartására és fejlesztésére, elvárva valamennyi munkatárs együttműködését.

A Társaság elkötelezett az iránt, hogy az általa biztosított szolgáltatásokat a legmodernebb technológiák felhasználásával, magas színvonalon, biztonságosan működő rendszerekkel lássa el, illetve az ehhez szükséges információbiztonsági folyamatokat és azokhoz szükséges megfelelő erőforrásokat (megoldásokat) biztosítsa annak érdekében, hogy alapfeladatai zavartalan ellátásához szükséges **adatkezelési, adatvédelmi és információbiztonsági** alapelvek minél magasabb szinten teljesüljenek.

A Társaság által kezelt (ügyfél/partner és személyes belső) adatok és információk összessége kiemelt értéket képvisel, melyet védeni kell, ezért törekszik arra, hogy ezek tekintetében folyamatosan teljesüljenek a bizalmassági, sértetlenségi, és rendelkezésre állási követelmények.

A Társaság tudatában van annak, hogy az általa nyújtott szolgáltatások, a működtetett rendszerek és az azokban feldolgozott adatok stratégiai jelentőségűek a megbízók, az ügyfelek számára, ezért a Társaság vezetése, minden munkatársa, és szerződéses partnere tevékenységét ennek megfelelő színvonalon és elkötelezettséggel végzi. A védelem szempontjából elkötelezett annak érdekében, hogy megakadályozza az illetéktelen behatolást, rendszerei feltörését, az illetéktelen hozzáférést, a szándékos vagy véletlen hibázást, károkozást.

Az üzletmenet folytonosságának biztosítása érdekében a Társaság a szükséges információvédelmi intézkedéseket megteszi, minden adatkezelési folyamatát az adatvédelmi és információbiztonsági elvárásoknak megfelelően alakítja ki.

A Társaság stratégiai céljai:

- A lehető legmagasabb szintű **ellátási minőség**, a szervezeti kultúra alapértékeként elfogadva;
- **Szervezeti fejlődés** (Triton szervezeti tudat, összetartás, hatékony koordináció kialakítása);
- **Integrált működés**;
- Gazdálkodási **eredményesség** fokozása;
- Kiemelt szakterületein **kiválósági központok** működtetése, akkreditáltatása;
- Országosan **vezető pozíciójú**, nemzetközileg **versenyképes**, magas minőségű egészségügyi magánellátás szolgáltatása.
- A vonatkozó nemzeti és nemzetközi **információbiztonsági törvényi/jogszabályi**, valamint az irányadó **szabványokban**, irányelvekben foglalt előírásoknak való maximális megfelelés, így különösen az **ISO 9001:2015**, **ISO/IEC 27001** és **MEEs** szabványban meghatározott információbiztonsági előírásoknak, irányelveknek való megfelelés.

A menedzsment feladatul határozta meg:

- az ellátó egységek szakmai tevékenységének **standardizálása** (a meglevő helyi sajátosságok, erőforrások figyelembevételével);
- **egységes**, valamennyi ellátó egységre és munkatársra érvényes cégcsoport-szintű **működési és dokumentációs elvek betartása**, nem kizárva előre egyeztetett és jóváhagyott helyi specifikumok alkalmazását;
- **minőségi ellátásra való törekvés** egyéni és szervezeti szinten;
- **munkatársak bevonása**, középvezetők elkötelezettségének megteremtése;
- **egységes dokumentációs rendszer és hierarchia kialakítása** – cégszintű közös és helyi speciális elemek;
- **koncentrált**, ugyanakkor hálózatos jellegű minőségirányítási működés;
- a társaság hagyományaihoz és hírnevéhez méltó, **korszerű, magas színvonalú betegellátás, biztonságos környezetben**, a kockázatok és a költségek optimalizálása mellett;
- elkötelezettség a **Minőségirányítási Egységes Rendszer** folyamatos fejlesztésére.

Célok elérésének eszközei:

- **szervezeti kultúra alapját képező közös szakmai értékrend**;
- a Társaság **egységes követelményrendszerének** fejlesztése és a működésben való alkalmazása, betartása és betartatása;
- **folyamatszemplélet** kialakítása;
- **belső szabályozások** egyértelműsítése;
- **munkafolyamatok, -eszközök és -eljárások standardizálása**;
- **egységes működési szabályozók és dokumentumok** kezelési rendjének kialakítása és működtetése;
- **felelősségi szintek és hatáskörök meghatározása és alkalmazása**, minden ellátó egységen, minden munkatársra;
- **csapaterőforrás-menedzsment**;
- **minőségközpontú szemlélet, magatartás és eredményesség** – alapvető követelmény a munkatársak, a beszállító, együttműködő szervezetek kiválasztásánál és a partneri kapcsolatokban is;

- tevékenység során használt **technológiák és a technikai eszközök** folyamatos **fejlesztése**;
- **munkatársak** képzettségének, szakmai tudásának, környezeti tudatosságának folyamatos és tervezett gyarapítása;
- tevékenységekhez kapcsolódó **anyag- és energia-felhasználás, valamint a hulladék és környezetkárosító anyagok kibocsátásának minimalizálása** a hasznosíthatósági lehetőségek kiaknázásával;
- **beszállítói struktúra optimalizálása**;
- komplex **kockázatértékelésen** alapuló rendszer működtetése, melynek elsődleges célja a lehetséges veszélyforrások és fenyegetettségek feltárása és értékelése. A biztonság fokozása érdekében megfelelő **információbiztonsági kontrollok** és korszerű informatikai megoldások alkalmazása;
- a következő **információbiztonsági működési alapelvek** folyamatos teljesülése:
 - a **védelem teljeskörűsége** alapelveként betartása, érvényesítése az összes rendszerelemre, a fizikai, logikai és az adminisztratív védelmi intézkedésekre is;
 - **zárttság** alapelveként belül biztosításra kerülnek és szerves egységet alkotnak a fenyegetések elleni védelmi intézkedések;
 - a **védelem kockázatarányosságának** alapelve – a védelem mértéke és költségei a kockázatokkal arányosak legyenek, célkitűzés a minimális költséggel elért maximális védelmi képesség;
 - a **védelem folytonosságának** alapelve – az informatikai rendszerek bevezetése során kialakított védelmi képességet a rendszer teljes életciklusa alatt folyamatosan biztosítani és fejleszteni szükséges.

Budapest, 2025. június 01.


Haraszi Péter György
vezérigazgató

