1. INTEGRÁLT MINŐSÉG-, KÖRNYEZET ÉS INFORMÁCIÓBIZTONSÁGI POLITIKA

Társaságunk, az **ITI Magyarország Kft. (ITI)** vezetőségének legfőbb célja– küldetése -, hogy **„Településfejlesztés [1]tanácsadási, [2]ágazati- és átfogó stratégiai dokumentumok, településfejlesztési koncepciók, programok és stratégiák/ okos város stratégiák készítése”** és egyéb kapcsolódó szolgáltatási tevékenységét úgy végezze, hogy azzal a **megrendelői** igényeknek, a **társadalmi** valamint a **hatósági** (jogszabályi, törvényi...) **elvárásoknak**, **szabályozásoknak** minél jobban megfeleljen, **környezetbarát** technológiai elemek/megoldások alkalmazására törekvő szolgáltatást nyújtva, elégedettségüket biztosítsa.

Elkötelezettek vagyunk az iránt, hogy az általunk biztosított szolgáltatásokat a legmodernebb technológiák felhasználásával, magas színvonalon, biztonságosan működő rendszerekkel lássuk el, illetve az ehhez szükséges információbiztonsági folyamatokat és azokhoz szükséges megfelelő erőforrásokat (megoldásokat) biztosítsuk annak érdekében, hogy alapfeladatainak zavartalan ellátásához szükséges **adatkezelési**, **adatvédelmi** és **információbiztonsági** alapelvek minél magasabb szinten teljesüljenek.

Az ITI által kezelt (ügyfél/partner és személyes belső) adatok és információk összessége kiemelt értéket képvisel, melyet védeni kell a különböző fenyegetések ellen, ezért törekszünkk arra, hogy ezek tekintetében folyamatosan teljesüljenek annak **bizalmassági**, **sértetlenségi**, és **rendelkezésre állási**[3] követelményei.

Tudatában vagyunk annak, hogy az általunk nyújtott szolgáltatások, a működtetett rendszerek és az azokban feldolgozott adatok stratégiai jelentőségűek a megbízók, az ügyfelek, a magyar önkormányzati szféra és tágabb értelemben a társadalom számára, ezért az ITI vezetése, minden munkatársa, és szerződéses partnere a munkájukat ennek megfelelő színvonalon és elkötelezettséggel kívánja végezni.

A védelem szempontjából folyamatosan tevékenykedünk annak érdekében, hogy megakadályozzuk az illetéktelen behatolást, a rendszereink feltörését, illetéktelen hozzáférését, a szándékos vagy véletlen hibázást, károkozást.

Az **üzletmenet folytonosság biztosítása** érdekében az ITI Magyarország a szükséges információvédelmi intézkedéseket megteszi, minden adatkezelési folyamatát az adatvédelmi és információbiztonsági elvárásoknak megfelelően alakítja ki.

Céljaink eléréséhez az alábbi vezetési eszközöket vesszük igénybe:

1. Társaságunk **fenti** tevékenységeire **kialakítjuk, működtetjük, és állandóan fejlesztjük az ISO 9001 és ISO 14001 szabványoknak megfelelő *minőségirányítási és környezetirányítási szabályozási rendszert*,** egy **minőség- és környezetorientált vezetési filozófia** meghonosítása érdekében.
2. **Kapcsolattartási rendszerünk fejlesztésével** *hosszú távú*, *korrekt ügyfél-, szállítói-, illetve hatósági szervezeti kapcsolatokat* alakítunk ki minden szolgáltatási területen, a társaság tevékenységéről az *érdekelt feleket* rendszeresen tájékoztatjuk.
3. Szolgáltatásaink minőségét a szükséges **erőforrások – személyi** (magas szintű szakismeret, szakképzettség, megfelelő tervezési jogosultságok…) **és egyéb** (tárgyi feltételek, folyamatos költségfigyelés…)**- biztosításával**, **a megrendelők és egyéb érdekelt felek igényeinek rugalmas kezelésével, a munkavégzés vezetői ellenőrzésével, a vevői, megrendelői észrevételek, panaszok gyors-rugalmas kezelésével valamint ezek tapasztalatainak a munkafolyamatokba történő visszacsatolásával, valamint az irányítási rendszer előírásainak betartásával biztosítjuk.**

[1] Stratégiai és üzletviteli tanácsadás
[2] Például: Fenntartható energia, klíma akcióterv; zöld infrastruktúra-fejlesztési terv, ITS, FVS stb.
[3] **1. Bizalmasság:** az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
2. Sértetlenség: a tárolt adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), a származás ellenőrizhető, megállapítható (letagadhatatlanság), illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
3. Rendelkezésre állás: az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók.

4. Tevékenységeink megtervezésénél fontosnak tartjuk a **környezeti feltételek/tényezők elemzését**, a lehetséges **vevő/megrendelői kör pontos ismeretét**, **bővítési**, **teljessé tételi lehetőségeit**, illetve a **személyes kapcsolattartásból származó információkat, melyek eredményeit folyamatszemléletű és kockázatalapú megközelítés alkalmazásával hasznosítjuk stratégiai döntéseinkben, működésünkben**.
5. Stabil vevőkapcsolataink érdekében, szolgáltatásaink esetén mindig biztosítjuk a **minőség-, *egyéb érdekeltek vonatkozásában pedig tevékenységeinkhez kapcsolódóan a környezeti szempontok, illetve szabályozások pontos betartását,* a korrekt pénzügyi elszámolást**.
6. Hasonló módon gondolkodunk a **partnereinkkel, beszállítóinkkal/alvállalkozóinkkal (szállítóinkkal)** kapcsolatban is, hiszen vevőink/megrendelőink magas szintű kiszolgálása csak úgy képzelhető el, ha stabil, szállítói háttérrel rendelkezünk, velük szorosan együttműködve dolgozunk, törekedve arra, hogy Ők is elégedettek legyenek.
7. Működésünk és a nyújtott szolgáltatások teljesítése során elkötelezettek vagyunk a vonatkozó nemzeti és nemzetközi **információbiztonsági törvényi/jogszabályi**[4], valamint az irányadó **szabványokban**, irányelvekben foglalt előírásoknak való maximális megfelelés iránt, így különösen az ISO/IEC 27001 szabványban meghatározott előírásoknak, irányelveknek való megfelelés iránt.
8. Komplex **kockázatértékelésen** alapuló rendszert működtetünk, melynek elsődleges célja a lehetséges veszélyforrások és fenyegetettségek feltárása és értékelése. A biztonság fokozása érdekében megfelelő **információbiztonsági kontrollokat**, és korszerű informatikai megoldásokat alkalmazunk.
9. Az alkalmazott, bevezetett **információbiztonsági kontrollokat** és azok működtetésének módját **ALKALMAZÁSI/ALKALMAZHATÓSÁGI NYILATKOZAT**-ban rögzítettük.
10. Biztosítjuk, hogy **POLITIKÁNKAT** szervezetünk minden szintjén **megértsék, elfogadják, és munkatársainktól** (beleértve a kapcsolódó partneri tevékenységekben közreműködőket) **elvárjuk a megfogalmazott alapelveknek megfelelő viselkedést**.
11. Ugyanakkor törekszünk arra, hogy munkatársaink természetes igényévé váljon a **minőségi és környezetorientált szempontokat is figyelembe vevő munkavégzés**, a **kezdeményezés a minőség és a környezti állapotok javítására**, melyhez minden feltételt biztosítunk számukra, beleértve:
    - az egyértelmű szervezeti felépítést és feladatlebontást, az ehhez rendelt világos döntési szinteket, az ennek megfelelő önállóságot és felelősségvállalást, megfelelő kommunikációs csatornákat a felső vezetéssel;
    - stabil munkahelyet, jó munkahelyi légkört és munkafeltételeket, eszközöket (beleértve a jogtiszta szoftvereket is)
    - a folyamatos szakmai, irányítási rendszer elemeivel kapcsolatos és egyéb képzést és továbbképzést,
    - a Társaság működésének (folyamat- és szolgáltatásparaméterek…) értékeléséről való rendszeres tájékoztatást
12. Dolgozóink, megbízóink, partnereink és a közvélemény elvárásainak való megfelelés érdekében kiemelt figyelmet fordítunk:
    - tevékenységeink **környezeti hatásának** vizsgálatára, jelentős (negatív) környezeti hatásaink mérséklésére, környezetre pozitív hatással lévő tevékenységeink, működési elemeink erősítésére, hangsúlyosabbá tételére
    - munkahelyi környezetünk **esztétikai** hatásának, felszereltségének javítására és

[4] **Nemzetközi szabályozások** tekintetében a *2016/679 (EU) Európai parlament és tanács rendelete (Európai Unió Általános Adatvédelmi Rendelete)*, illetve a *GDPR rendelet* - **nemzeti szabályozások** tekintetében pedig a *2011. évi CXII törvény az Információs önrendelkezési jogról és információszabadságról*, illetve az ügyfélkörre való tekintettel a *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról…* a legfontosabb szem előtt tartott jogszabályi követelmények.

- a következő **információbiztonsági működési alapelvek** folyamatos teljesülésére:
    1. A **védelem teljes körűségének** alapelvét be kell tartani. Az elvet érvényesíteni kell az összes rendszerelemre, a fizikai, logikai és az adminisztratív védelmi intézkedésekre is.
    2. **Zártság** alapelvén belül biztosítani kell, hogy a fenyegetések ellen meglévő védelmi intézkedések megvalósításra kerültek és azok szerves egységet alkotnak.
    3. A **védelem kockázatarányosságának** alapelve, hogy a védelem mértéke és a költségei a kockázatokkal arányosak legyenek. Célkitűzés a minimális költséggel elért maximális védelmi képesség.
    4. A **védelem folytonosságának** alapelve, hogy az informatikai rendszerek bevezetése során kialakított védelmi képességét a rendszer teljes életciklusa alatt folyamatosan biztosítani és fejleszteni kell.

13. Szolgáltatásaink biztonságos színvonaltartását irányítási rendszerünk **folyamatos ellenőrzésével, teljesítéseink, eredményeink mérhető értékelése alapján megtervezett fejlesztésével,** és **az esetlegesen előforduló nemmegfelelőségek, incidensek, események figyelésével, javításával** is garantáljuk.
14. Az adatvédelmi eseményeket, **incidenseket**, az információbiztonsági nem megfeleléseket minden esetben kivizsgáljuk, és szükséges korrekciós intézkedéseket bevezetjük, illetve az ezekből nyert tapasztalatokat hasznosítjuk az információbiztonság hatékonyságának fejlesztése érdekében.

A jövőre gondolva elhatározott szándékunk, hogy szolgáltatásaink, *tevékenységeink* színvonaltartásával, illetve folyamatos fejlesztésével, tevékenységbe bevont külső partnereinkkel és megrendelőinkkel szorosan együttműködve, megbízható, közel panaszmentes, biztonságos szolgáltatást nyújtsunk...