

BESZÁLLÍTÓKRA VONATKOZÓ CITI-KÖVETELMÉNYEK

TULAJDONOSOK:

A Citi globális beszerzési és kockázati részlegének vezetője

KIÁLLÍTÁS DÁTUMA:

2015. január

FELÜLVIZSGÁLAT:

2026. szeptember

VERZIÓ:

9

TARTALOMJEGYZÉK

1	ÁLTALÁNOS ÁTTEKINTÉS.....	3
2	ESÉLYEGYENLŐSÉG A FOGLALKOZTATÁSBAN	5
3	VESZTEGETÉS ÉS KORRUPCIÓ ELLENI KÜZDELEM	6
4	AJÁNDÉKOK ÉS SZÓRAKOZTATÁS	7
5	BESZÁLLÍTÓI EGYÜTTMŰKÖDÉSI ÉS BESZÁLLÍTÓI ALAPELVEK	7
6	MODERN RABSZOLGASÁGRA VONATKOZÓ TILALOM	8
7	A BESZÁLLÍTÓ SZEMÉLYZETE	10
8	CSALÁSOK KEZELÉSE	12
9	MÉDIA KERETEIN BELÜLI INTERAKCIÓK ÉS NYILVÁNOS MEGJELENÉSEK.....	13
10	ELEKTRONIKUS ÍRÁSBELI KOMMUNIKÁCIÓ	14
11	POLITIKAI TEVÉKENYSÉGEK ÉS HOZZÁJÁRULÁSOK	15
12	PÉNZMOSÁS-ELLENESSÉG („AML”)	16
13	NYILVÁNTARTÁSOK KEZELÉSE	18
14	VÁLLALATI RUGALMASSÁGI/ÜZLETMENET-FOLYTONOSSÁG	19
15	GLOBALIS HÁTTÉR-ÁTVILÁGÍTÁSI SZABVÁNYOK	26
16	KÖLTSÉGEK	28
17	INFORMÁCIÓBIZTONSÁG (IS).....	29
18	MUNKAHELYI BIZTONSÁGGAL KAPCSOLATOS IRÁNYMUTATÁSOK	68
19	MESTERSÉGES INTELLIGENCIA/GÉPI TANULÁS (BELEÉRTVE A GENERATÍV MESTERSÉGES INTELLIGENCIÁT ÉS AZ AUTONÓM ÜGYNÖK ALAPÚ MESTERSÉGES INTELLIGENCIÁT IS).....	70
20	ÜGYFÉLPANASZOK	71
21	SZEMÉLYES KERESKEDELMI ÉS BEFEKTETÉSI SZABÁLYZAT	72
22	SZÁMLÁZÁS ÉS SZÁMLÁZÁSI SZABVÁNYOK.....	72
23	KÖTELEZŐ TÁVOLLÉTI IRÁNYELV	73
	FÜGGELÉK – FOGALOMMEGHATÁROZÁSOK	74

1 ÁLTALÁNOS ÁTTEKINTÉS

1.1. Általános követelmények

Ezek a Beszállítókra vonatkozó Citi-követelmények („**Követelmények**”) részletezik azon kötelezettségek egy részét, amelyeket a Beszállítóknak teljesíteniük kell a Citivel folytatott üzleti tevékenységeik során. Bizonyos Követelmények minden Beszállítóra vonatkoznak, míg más követelmények egy adott Beszállítóra való alkalmazhatósága a Beszállító által a Citi számára biztosított termék(ek)től és szolgáltatás(ok)tól függ (ez utóbbiakat az alábbi 1.2 fejezet foglalja össze, és az ott felsorolt egyes rendelkezések elején vannak feltüntetve). A nagybetűs kifejezések a jelen dokumentumban, illetve az ahhoz csatolt Függelékben meghatározott jelentéssel bírnak, kivéve, ha jelen dokumentumban ilyen jelentés nincs feltüntetve; utóbbi esetben a kifejezések a Szerződésben meghatározott jelentéssel bírnak, az alábbiakban meghatározottak szerint.

Ezek a Követelmények a Citivel kötött Beszállítói megállapodások (többek között, de nem kizárólagosan a tranzakciós dokumentumok, pl. munkamegrendelések, engedélyezési ütemtervek) (külön-külön „**Szerződés**”) szerinti szerződéses kötelezettségek, és kiegészítésként szolgálnak bármely egyéb Megállapodásban előírt kötelezettséghez, az Alkalmazandó Jogszabályok által előírt bármely kötelezettséghez (a kifejezés alábbi meghatározása alapján), a Citi által a Beszállítónak küldött bármely értesítéshez, amelyben tájékoztatja a Beszállítót az abból eredő kötelezettségekről (külön-külön „**Értesítés**”), vagy a Citi üzletvitele és tevékenységei tekintetében alkalmazott bármely további, konkrétabb követelményhez. Amennyiben a fenti követelmények és e követelmények között bármiféle ellentmondás merül fel, a szigorúbb kötelezettségek és követelmények alkalmazandók. A Beszállítóknak proaktív szerepet kell vállalniuk, és konzultálniuk kell elsődleges Citi üzleti kapcsolattartójukkal (vagy kijelölt kapcsolattartójukkal) a jelen Követelményekkel kapcsolatban felmerült kérdéseikről, beleértve a Követelmények bármely módosítását, a mentesítési kérelmeket, illetve a Követelmények előírásai közötti vagy az Alkalmazandó Jogszabályokkal való vélt összeférhetlenségeket.

A Beszállító haladéktalanul eleget tesz minden olyan észszerű kérésnek, amelyet a Citi olyan adatokkal kapcsolatban nyújt be a Beszállítóhoz, amely adatokat a Citi az Alkalmazandó Jogszabályok betartására vonatkozó kötelezettsége miatt igényel a Beszállító Szolgáltatásaival és Személyzetével kapcsolatban. Ha a Beszállító nem tesz eleget ezen kötelezettségeinek, az a jelen Szerződésben foglalt feltételek lényeges megszegésének minősül.

A jelen Követelmények vagy bármely, a Beszállítóval üzleti tevékenységet folytató Citi vállalat által meghatározott további követelmény be nem tartása a Beszállító Citivel kötött szerződésének felbontását vonhatja maga után. A Követelmények megszegése továbbá az Alkalmazandó Jogszabályok megsértését is jelentheti, mely a Citire (vagy harmadik felekre) nézve polgári kártérítési eljárásokat vagy a Beszállítóra nézve büntetőjogi szankciókat vonhat maga után. A Beszállító a Citi írásbeli hozzájárulása nélkül nem jogosult figyelmen kívül hagyni jelen Követelmények előírásait a saját szabályzatainak való megfelelésre hivatkozva.

1.2. Egyes Beszállítókra vonatkozó Követelmények

Az alábbi táblázat olyan Követelményeket határoz meg, amelyek az itt megadott alkalmazhatósági kritériumoknak megfelelő Beszállítókra vonatkoznak. Az alább nem említett fejezetek MINDEN Beszállítóra vonatkoznak.

Fejezet száma	Fejezet címe	Alkalmazhatóság
2	ESÉLYEGYENLŐSÉG A FOGLALKOZTATÁSBAN / MEGERŐSÍTŐ INTÉZKEDÉSEK	Az Egyesült Államok szövetségi kormányával kötött Citi-szerződés teljesítéséhez szükséges szerződésekre és megrendelésekre alkalmazandók. Amennyiben nem egyértelmű, hogy az adott szerződés vagy megrendelés szövetségi kormányzati alvállalkozói szerződésnek vagy megrendelésnek minősül-e, a záradék elején vagy végén – az adott szöveggörnyezetnek megfelelően – fel kell tüntetni az „Amennyiben alkalmazandó” megjelölést.
12	PÉNZMOSÁS-ELLENESSÉG	Azokra a Beszállítókra vonatkozik, akik bizonyos ügyféllel kapcsolatos szolgáltatásokat (pl. bevezetés, ügyfélszámla és tranzakciók átvilágítása) nyújtanak, vagy amelyek az előbbi tevékenységekkel kapcsolatban adatokat/mutatókat biztosítanak; <u>ÉS/VAGY</u> Azokra a Beszállítókra, akik közvetítőként járnak el készpénzzel vagy pénzügyi eszközökkel kapcsolatban (pl. távoli letét felvétele, futár, páncéljármű és széf szolgáltatások).
13	NYILVÁNTARTÁSOK KEZELÉSE	Azokra a Beszállítókra vonatkozik, akik elérlik/feldolgozzák/tárolják a Citivel kapcsolatos információkat.
14	ÜZLETMENET-FOLYTONOSSÁG	Azokra a Beszállítókra vonatkozik, akik a Citi által használt szolgáltatásokat nyújtanak, vagy ilyen technikai jellegű infrastruktúrát/alkalmazásokat üzemeltetnek. A Citi által kijelölt üzleti tevékenységért felelős személy (BAO) felelőssége tájékoztatni a Beszállítót az alkalmazhatóságról és az üzletfolytonossági követelményekről.
15	GLOBALIS HÁTTÉR-ÁTVILÁGÍTÁSI SZABVÁNYOK	Azokra a Beszállítókra vonatkoznak, akik szolgáltatásokat nyújtanak a Citinek.
16	KÖLTSÉGEK	Azokra a Beszállítókra vonatkoznak, akik szerződés alapján jogosultak visszatérítendő üzleti költségek igénylésére.
17	INFORMÁCIÓBIZTONSÁG (IS)	Azokra a Beszállítókra – beleértve az Alvállalkozókat is – alkalmazandó, amelyek hozzáférnek a Citi információihoz, azokat feldolgozzák, kezelik vagy tárolják; <u>ÉS/VAGY</u> a Citi márkajelzésével ellátott, internetről elérhető alkalmazások tárhelyszolgáltatójaként felelősek azok üzemeltetéséért; <u>ÉS/VAGY</u> kapcsolódnak a Citi hálózati erőforrásaihoz; <u>ÉS/VAGY</u> kíséret nélküli hozzáférést igényelnek a Citi létesítményeihez.
18	MUNKAHELYI BIZTONSÁGGAL KAPCSOLATOS IRÁNYMUTATÁSOK	

Fejezet száma	Fejezet címe	Alkalmazhatóság
19	MESTERSÉGES INTELLIGENCIA/GÉPI TANULÁS (beleértve a generatív mesterséges intelligenciát és az autonóm ügynök alapú mesterséges intelligenciát is)	Azokra a Beszállítókra alkalmazandó, amelyek a Citi meghatározása szerinti mesterséges intelligenciát vagy gépi tanulást (AI/ML) alkalmaznak az általuk nyújtott termék vagy szolgáltatás bármely elemében.
20	SZEMÉLYES KERESKEDELMI ÉS BEFEKTETÉSI SZABÁLYZAT	Azokra a Beszállítókra vonatkozik, akik a Citinél betöltött munkaköri feladataik részeként rendszeres hozzáférést igényelnek nem nyilvános lényegi információhoz.
23	KÖTELEZŐ TÁVOLLÉTI IRÁNYELV	Ez az Irányelv alkalmazandó azokra a nem munkaviszonyban álló személyekre (a továbbiakban: „Munkavállalók”), akik Érzékeny Munkakört töltenek be (a Szószedet meghatározása szerint) (a továbbiakban: „Érzékeny Munkavállalók”), továbbá az Érzékeny Alkalmazottak közvetlen vezetőire és irányítóira (a továbbiakban: „Vezetők”), valamint az Érzékeny, nem munkaviszonyban álló személyek Citi üzleti kapcsolattartóira.

2 ESÉLYEGYENLŐSÉG A FOGLALKOZTATÁSBAN

2.1 Esélyegyenlőség a foglalkoztatásban.

A Citi olyan irányelveket alakított ki, amelyek célja, hogy valamennyi megfelelő képesítéssel rendelkező személy számára biztosítsák a foglalkoztatás során az esélyegyenlőséget, faji vagy etnikai hovatartozástól, bőrszíntől, vallástól, nemtől, szexuális irányultságtól, nemi identitástól, nemzeti származástól, állampolgárságtól, bevándorlási jogállástól, életkortól, családi állapottól, genetikai információktól, fogyatékosságtól, védett veterán státusztól vagy bármely más, jogszabály által védett tulajdonságtól függetlenül.

A Beszállítók kötelesek megfelelni, és gondoskodni róla, hogy személyzetük is teljesítse az összes vonatkozó megkülönböztetés elleni törvény és szabályozás követelményét, beleértve, a teljesség igénye nélkül, minden olyan törvényt és szabályozást, amelynek tekintetében a Citi írásban tájékoztatja a Beszállítót a megfelelőségi követelményről.

A Beszállítók kötelesek megismerni a Citi U.S. Equal Employment Opportunity Policy Statement irányelvének előírásait, és azzal összhangban megtenni a megfelelő intézkedéseket. Az irányelv az alábbi címen érhető el: www.citigroup.com/global/eeo-aa-policy.

2.2 Állami szerződések

A szövetségi kormányral kötött Citi-szerződések teljesítéséhez szükséges szerződéseknek és beszerzési megrendeléseknek szó szerint tartalmazniuk kell az alábbi bekezdést, félkövér betűkkel, az alábbiak szerint. (Ha nem biztos abban, hogy szövetségi kormányral kötött alvállalkozói szerződésről/beszerzési megrendelésről van-

e szó, akkor óvatosságból írja bele az alábbi pontot, és kezdje azt az „Amennyiben alkalmazható” kifejezéssel.)

[Amennyiben alkalmazható,] A Beszállító köteles betartani az összes vonatkozó szövetségi diszkriminációellenes törvényt, és igazolni, hogy nem működtet az alkalmazandó szövetségi diszkriminációellenes törvényeket sértő programokat

2.3 Állami szerződésekre vonatkozó függelék

A szövetségi kormányral kötött Citi-szerződés teljesítéséhez szükséges szerződéseknél és beszerzési megrendeléseknek tartalmazniuk kell a következő értesítést az alvállalkozói szerződés vagy a beszerzési megrendelés függelékében. (Ha nem biztos abban, hogy szövetségi kormányral kötött alvállalkozói szerződésről/megbízásáról van-e szó, akkor óvatosságból írja bele az alábbi nyilatkozatot, és zárja azt az „Amennyiben alkalmazható” kifejezéssel.)

A Citigroup, mint a szövetségi kormány szerződéses beszállítója, ezúton írásban értesíti az alulírott vállalkozót vagy forgalmazót azokról az esélyegyenlőségi intézkedésekről, amelyeket a védett veteránok és a fogyatékkal élők érdekében köteles meghozni. A Citigroup teljes mértékben megfelel a rehabilitációról szóló törvény 503. szakaszának, a vietnami háborús veteránok beilleszkedését elősegítő törvénynek, valamint annak a 41 C.F.R. § 60-741, illetve a 41 C.F.R. § 60-300 szerinti vonatkozó előírásainak. Equal Employment Opportunity Policy Statement irányelvünk a www.citigroup.com/global/eeo-aa-policy weboldalon található. Ha az egyenlő foglalkoztatási esélyekre vonatkozó irányelvről szóló nyilatkozatunkkal kapcsolatban kérdése merülne fel, akkor forduljon a nyilatkozatban megadott kapcsolattartó személyhez.

[Amennyiben alkalmazható] Kérjük, tegye meg a megfelelő intézkedéseket az irányelvre vonatkozó nyilatkozattal, valamint az előírásokkal összhangban.

3 VESZTEGETÉS ÉS KORRUPCIÓ ELLENI KÜZDELEM

A Citi olyan irányelvekkel, eljárásokkal és belső ellenőrzésekkel rendelkezik, amelyek észszerűen úgy vannak kialakítva, hogy megfeleljenek a vonatkozó vesztegetés- és korrupcióellenes törvényeknek; továbbá a Citi szigorúan tiltja a vesztegetést és a könnyítő kifizetéseket is. A Beszállítók (ideértve az Üzletszerzőket is), azok Személyzete és bárki, aki közvetlenül vagy közvetve a Citi nevében jár el, köteles tevékenységét a legmagasabb etikai normák szerint, valamint az Egyesült Államok külföldi korrupciós gyakorlatokkal kapcsolatos törvényének (FCPA), az Egyesült Királyság vesztegetési törvényének (UKBA) és azok módosításainak megfelelően folytatni, valamint köteles betartani az abban az országban érvényes összes egyéb vonatkozó helyi vesztegetés- és korrupcióellenes törvényt, ahol a Citi tevékenységét végzi.

Sem a Beszállító sem a Beszállító Személyzetének azon tagjai, akik a Citi nevében vagy a Beszállítónak a Citivel kötött szerződésével vagy kapcsolatával összefüggésben járnak el (i) nem biztosíthatnak, engedélyezhetnek vagy ajánlhatnak fel semmilyen kifizetést, hasznot, előnyt vagy bármilyen más értéket senkinek, és senkivel nem tárgyalhatnak ezekről; (ii) nem vehetnek át vagy fogadhatnak el senkitől semmilyen kifizetést, hasznot,

előnyt vagy bármilyen más értéket, amennyiben az (i)-(ii) egyes esetei sértik az FCPA-t, az UKBA-t vagy bármely más vesztegetés- és korrupcióellenes törvényt. A Beszállító és Személyzetének tagjai kötelesek úgy végrehajtani a Citi nevében vagy a Beszállítónak a Citivel kötött szerződésével vagy kapcsolatával összefüggésben végzett tevékenységeiket és tranzakcióikat, hogy azok megfeleljenek a Követelményeknek, beleértve jelen Fejezetet is. A Beszállító és annak Személyzete továbbá köteles fenntartani egy vesztegetés- és korrupcióellenes megfelelőségi programot, valamint olyan irányelveket és eljárásokat, amelyeket úgy alakítottak ki és alkalmaznak, hogy azok biztosítsák az összes vesztegetés- és korrupcióellenes törvénynek való megfelelést.

A Citi vesztegetés- és korrupcióellenes programjának áttekintéséhez látogasson el a következő oldalra: [Citigroup's Investor Relations](#) (a Citi irányelvei alatt válassza az AB&C Program lehetőséget).

4 AJÁNDÉKOK ÉS SZÓRAKOZTATÁS

Sem a Beszállítók, sem a Beszállítók Személyzetének tagjai nem adhatnak ajándékokat vagy más értéket (beleértve a szórakoztatást is) a Citi alkalmazottainak, amennyiben ez tényleges vagy látszólagos érdekellentétet vagy ellenszolgáltatást teremtene, kompromittálná az alkalmazott integritását vagy ítélőképességét vagy egyéb módon nem helyénvalóan befolyásolná a döntéshozatalát, hatására az alkalmazott kötelezettségeivel ellentétesen cselekedne, vagy ha az egyéb módon sértené a vonatkozó törvényeket. A fentiek korlátozása nélkül az alkalmazott köteles betartani az ajándékokra és szórakoztatásra vonatkozó szabványban foglalt tiltott ajándékokra és szórakoztatásra vonatkozó részt. A Beszállítók és a Beszállítók Személyzetének tagjai személyenként és naptári évenként összesen maximum 300 amerikai dollár értékben adhatnak nem készpénzbeli üzleti ajándékot a Citi alkalmazottainak.

Amikor egy Beszállító üzleti szórakoztatást biztosít a Citi egyik alkalmazottja számára (pl. étkeztetést, sport-, kulturális vagy más hasonló eseményekre való meghívást), akkor a Beszállítónak is részt kell vennie az eseményen, és a szórakoztatásnak helyénvalónak, a szokásoknak megfelelőnek és észszerűnek kell lennie, nem lehet pazar vagy túlzottan gyakori. Továbbá, ha a Beszállító nem vesz részt az eseményen, akkor a szórakoztatás üzleti ajándéknak minősül, és a Citi ajándékokra és szórakoztatásra vonatkozó szabványában foglalt vonatkozó jelentéstételi küszöbértékek érvényesülnek. A Beszállító ténylegesen vagy állítólagosan a Citi nevében eljárva sem közvetlenül, sem közvetve nem nyújthat semmilyen értéket senkinek (akár a Beszállító saját költségén, akár a Citi alkalmazottjának költségén), illetve nem ösztönözhet mást erre, ha az ténylegesen korrupciós, nem megfelelő vagy a vonatkozó jogszabályokat sértő lenne, vagy ha arról észszerűen feltételezhető lenne ezek bármelyike.

5 BESZÁLLÍTÓI EGYÜTTMŰKÖDÉSI ÉS BESZÁLLÍTÓI ALAPELVEK

<https://www.citigroup.com/citi/suppliers/>A Citi számos kezdeményezés keretében működik együtt Beszállítóival, valamint ismerteti beszerzési programját azokkal a

potenciális Beszállítókkal, amelyek az általa kiszolgált közösségekből kerülnek ki. Ezek az együttműködések emellett segítenek azonosítani az ígéretes Beszállítókat, különösen azokat, amelyek innovatív megoldásokat kínálnak a felmerülő üzleti kihívások kezelésére. A Citi Beszállítókkal szembeni elvárásairól további információ az [\[u\]Doing Business with Citi](#) weboldalon érhető el, a következő címen:

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 MODERN RABSZOLGASÁGRA VONATKOZÓ TILALOM

A Citi elkötelezte magát az olyan gyakorlat mellett, amely célja a modern rabszolgaság és emberkereskedelem előfordulási kockázatának azonosítása és kezelése a szervezetén belül vagy az ellátási láncában. A Citi Beszállítói kötelesek betartani az alábbiakban meghatározott Követelményeket, és hatékony, az egész vállalatra kiterjedő irányelveket és/vagy eljárásokat kidolgozni a modern rabszolgaság és emberkereskedelem kockázatának azonosítására és megelőzésére a saját tevékenységük és ellátási láncaik keretein belül. A Beszállítóknak a Citi kérésére ki kell tölteniük a Citi vállalati felelősségvállalással kapcsolatos kérdőívét, beleértve az esetlegesen szükséges kiegészítő információkat is, hogy a Citi felmérhesse a kockázatnak való kitettséget és a lehetséges kockázatcsökkentő lépéseket, különösen a magasabb kockázatú szektorokban és földrajzi területeken működő Beszállítók esetében. A Beszállító Alvállalkozóitól elvárjuk, hogy ugyanezt a folyamatot kövessék.

6.1 Gyermekmunka elkerülése

A Beszállítók nem alkalmazhatnak gyermekmunkásokat. A „gyermek” kifejezés minden olyan személyt magába foglal, aki az alkalmazandó jogszabályok szerint még nem érte el a foglalkoztatás alsó korhatárát, illetve ilyen jogszabály hiányában minden olyan személyt, aki nem töltötte be a 15. életévét vagy nem fejezte be a tankötelezettséget – attól függően, hogy e két korhatár közül melyik a magasabb. Ha 18 év alatti munkavállalókat alkalmaznak, akkor, a gyermekmunka alkalmazásának átfogó tilalmát figyelembe véve, különös gondot kell fordítani feladatköreikre és a munkavégzés körülményeire, így biztosítandó, hogy munkájuk vagy munkakörülményeik közvetlen vagy közvetett eredményeként ne érje őket fizikai, mentális vagy egyéb kár.

6.2 Szabadon választott munkavállalás

A Beszállító köteles biztosítani, hogy a munkavállalók ne álljanak mentális vagy fizikai kényszer alatt, ne legyen rájuk kényszerítve rabszolgaság vagy adósrabszolgaság, ne kötelezzék őket szerződésre, ne végeztesse velük akaratuk ellenére börtönmunkát, ne legyenek rabszolga-kereskedelem áldozatai, és ne végezzenek semmilyen formában kötelező munkát, beleértve a kényszerű túlórákat is. Minden munkát önkéntesen kell elvégezni. A Beszállító jelen dokumentumban meghatározott kötelezettségei, a teljesség igénye nélkül:

1. **Szerződések, bérek és munkaidő:** A munkavállalók foglalkoztatási vagy megbízási feltételeit olyan írásos dokumentumban kell rögzíteni, amely

könnyen érthető számukra, és amely egyértelműen meghatározza jogait és kötelezettségeiket. Ennek az írásos dokumentumnak mindenképpen, de nem kizárólagosan tartalmaznia kell a következőkre vonatkozó átlátható feltételeket: bérek, túlóradíjak, kifizetési időszakok, munkaidő, valamint a szünetekre és szabadnapokra vonatkozó jogok. Az ilyen írásbeli feltételeket a munkavállalónak a munkaviszony megkezdése előtt át kell adni, a munkáltatónak tiszteletben kell tartania azokat, és meg kell felelniük az iparági szabványoknak és a munkavégzés helyén alkalmazandó törvények és kollektív szerződések minimumkövetelményeinek.

2. **A munkaviszony szabad megszüntetésének joga:** A munkavállalóknak jogosultnak kell lenniük szabadon megszüntetni munkaviszonyukat, adott esetben az alkalmazandó törvényekkel és kollektív szerződésekkel összhangban lévő, észszerű felmondási idő elteltével, és bármilyen jogtalan büntetés kiszabása nélkül.
3. **Embertelen bánásmód:** A munkavállalókat, családtagjaikat és a velük szoros kapcsolatban állókat tilos durva vagy embertelen bánásmódnak kitenni, beleértve, a teljesség igénye nélkül, a fizikai fenyegetést, a fizikai, pszichológiai és szexuális erőszakot és kényszerszert, a szóbeli bántalmazást, a zaklatást és a megfélemlítést. A vendégmunkásokat, családtagjaikat és a velük szoros kapcsolatban állókat nem szabad nemzetiségük miatt megkülönböztetni a munkafeltételek és -körülmények tekintetében.
4. **Bérek, juttatások és munkaidő:** A kompenzációnak meg kell felelnie az összes vonatkozó bértörvénynek, beleértve a minimálbérré, a túlórákra és a törvényileg előírt juttatásokra vonatkozókat is. A munkavállalók részére a munkabért teljes összegben, határidőben és átlátható bérjegyzékkel együtt kell kifizetni. Fegyelmi intézkedésként tilos a munkabérből vagy a juttatásokból büntető jellegű levonást alkalmazni, illetve azok kifizetését visszatartani. A munkahét időtartama nem haladhatja meg a helyi jogszabályokban meghatározott felső határt. A túlmunka kizárólag önkéntes alapon, a jogszabályi keretek között végezhető, és a túlmunka vállalásának megtagadása miatt a munkavállalót semmilyen hátrány nem érheti.
5. **Tilos a személyazonosító okmányokat elkobozni:** A munkavállalóktól a foglalkoztatás feltételeként nem kobozhatják el vagy tarthatják vissza személyazonosító dokumentumaikat, utazási engedélyüket, útlevelüket vagy más hivatalos okmányaikat, illetve bármely más értéktárgyukat; a tulajdon visszatartása nem használható fel a munkavállalók szabadságjogainak közvetlen vagy közvetett korlátozására vagy munkahelyi rabszolgaság létrehozására.
6. **Tilos a munkaközvetítési díj és az adósságrabszolgaság:** A munkavállalók toborzásával kapcsolatos díjak és költségek (beleértve, a teljesség igénye nélkül, a munkavállalói vízumokkal kapcsolatos díjakat, az utazási költségeket és a dokumentumfeldolgozási költségeket) nem számíthatók fel a munkavállalóknak, sem közvetlenül, sem közvetve. Hasonlóképpen a

munkavállalók nem kötelesek olyan kifizetések teljesítésére, amelyek célja munkahelyi rabszolgaság létrehozása, vagy amelyek annak létrejöttét eredményezik, ideértve a biztosíték fizetését, valamint nem kötelezhetők adósság munkával történő visszafizetésére. Ha megállapítást nyer, hogy a munkavállalókra a toborzási folyamattal összefüggésben, illetve a foglalkoztatásuk során díjakat vagy költségeket hárítottak át, a Beszállító köteles észszerű intézkedéseket tenni annak érdekében, hogy e költségek a munkavállalók részére haladéktalanul megtérítésre kerüljenek. Ha olyan munkavállalókat kell toborozni, akiket harmadik félen, például munkaerő-közvetítőn keresztül foglalkoztatnak, akkor kizárólag jó hírnévvel rendelkező munkaerő-közvetítő irodák vehetők igénybe. Ha a munkavállalók keresése közvetlen foglalkoztatás céljából történik, akkor kizárólag jó hírnévű munkaerő-toborzó irodák vehetők igénybe. A munkavállalók által fizetett toborzási díjak tilalma valamennyi toborzóra, ügynökre és alügynökre kiterjed. A Beszállítóknak megfelelő belső kontrollokat kell működtetniük a követelmények betartásának biztosítása érdekében. **Munkavállalók szabad mozgása:** A munkavállalók jogosultak szabadon, indokolatlan korlátozások nélkül mozogni, nem szabad mozgásukat fizikailag a munkahelyükre vagy más, a munkáltató által ellenőrzött helyszínekre (például szálláshelyekre) korlátozni. A munkavállalókkal szemben nem követelhető meg, hogy a munkáltató által ellenőrzött szállásokon szálljanak meg, kivéve, ha erre az elvégzett munka helye vagy jellege miatt szükség van.

7. **Megtorlás nélküli panasztétel:** A munkavállalók jogosultak szabadon panaszt benyújtani a munkáltatójuknál annak velük szembeni bánásmódjával kapcsolatban; a panasztevő munkavállalókat nem szabad panaszuk miatt hátránnak, megtorlásnak vagy büntetésnek kitenni.

7 A BESZÁLLÍTÓ SZEMÉLYZETE

7.1 A Beszállító személyzetének képzése, beosztása, áthelyezése és irányítása

A Beszállító köteles a Szolgáltatások leghatékonyabb, a Szerződés előírásai szerinti elvégzéséhez megfelelő képzettséggel, végzettséggel, tapasztalattal és készségekkel rendelkező megfelelő számú személyt alkalmazni, és kérésre köteles igazolni az adott személyek képzettségét. Miután a Személyzetet már egy Projekthez rendelték, a Beszállító a Citi előzetes írásbeli hozzájárulása nélkül nem helyezheti át vagy bízhatja meg a Személyzetet más olyan feladatokkal, melyek csökkentik a Projekten való munkavégzésre való képességet; a Beszállító általában véve köteles a Projektekhez úgy beosztani a Személyzetet, hogy minimalizálja az átképzés szükségességéből adódó zavarokat. A Beszállító köteles biztosítani, hogy Személyzetének tagjai semmilyen célból ne tüntessék fel magukat a Citi alkalmazottjainak vagy képviselőinek, és ne követeljék, hogy a Citi alkalmazottjaiként kezeljék őket, beleértve a Citi által nyújtott béren kívüli juttatásokra, rokkantsági járadékokra, társadalombiztosítási adókra és juttatásokra, szövetségi munkanélküliségi adókra, állami munkanélküli-biztosítási járadékokra, és szövetségi jövedelemadó-levonásra vonatkozó igényeket is. A Beszállító kizárólagos

felelősséggel tartozik minden Személyzete felé való munkáltatói kötelezettségért, beleértve, a teljesség igénye nélkül, minden szükséges biztosítást, az összes vonatkozó adóbevallás benyújtását, valamint az összes szükséges adótartozás és -letét teljesítését, a Beszállító független vállalkozói státuszával összhangban.

7.2 A Beszállító Személyzetének leváltása

A Beszállító köteles eltávolítani és lecserélni az általa a Projekthez rendelt Személyzetet, ha a Citi értesíti, hogy az adott személy bármilyen megkülönböztetéssel össze nem függő okból nem elfogadható a Citi számára. A Beszállító ezenfelül vállalja, hogy haladéktalanul eltávolítja és lecseréli, illetve a Citinek biztosított Szolgáltatásoktól (vagy a Szolgáltatások nyújtásával vagy felügyeletével kapcsolatos bármilyen felelősségi körtől) eltiltja a Projekthez rendelt Személyzetet, ha nem képes vagy nem hajlandó a Szolgáltatásokat időben és szakszerűen teljesíteni.

7.3 A Beszállító Személyzetére vonatkozó irányelvek

A Beszállító kijelenti, szavatolja és kötelezettséget vállal arra, hogy átfogó szabályzatokat és eljárásokat tart fenn és alkalmaz hatékonyan a Citinek helyszíni Szolgáltatások nyújtására kijelölt természetes személyek minősítésére; ezek a szabályzatok és eljárások magukban kell, hogy foglalják a munkavállalási engedélyek ellenőrzését, a foglalkoztatási múlt és az esetleges büntetőjogi ítéletek háttér-átvilágítását, a jelen dokumentumban részletesebben ismertetett módon, valamint a foglalkoztatás előtti drogtesztet. Mindezt az Alkalmazandó jogszabályok és az alkalmazandó kollektív szerződések által megengedett mértékben kell megvalósítani. A Beszállító továbbá kijelenti, szavatolja és vállalja, a fentiek általános érvényének korlátozása nélkül, hogy rendelkezik olyan ellenőrzésekkel és eljárásokkal, melyek biztosítják a bevándorlással kapcsolatos Alkalmazandó jogszabályoknak való teljes megfelelést, beleértve annak ellenőrzését, hogy a Beszállító Citihez kirendelt teljes Személyzete jogosult dolgozni a megbízás teljes időtartama alatt, a bevándorlással kapcsolatos Alkalmazandó jogszabályoknak megfelelően. Kérésre a Beszállító köteles haladéktalanul írásos bizonyítékot adni a Citinek a Citihez rendelt Személyzet bármely vagy összes tagjának munkavállalási engedélyéről, valamint a bevándorlással kapcsolatos Alkalmazandó jogszabályoknak való megfeleléséről; a Beszállító ezenfelül köteles lecserélni és megfelelően képzett személyekkel helyettesíteni a Személyzet bármely olyan tagját, aki nem rendelkezik az Alkalmazandó jogszabályoknak megfelelő munkavállalási engedéllyel. Ennek keretében a Beszállító köteles biztosítani a Szolgáltatások időszerű és hatékony teljesítéséhez szükséges összes képzést és tájékoztatást, a Citi számára minden további költség felszámítása nélkül.

7.4 Beszállítói tulajdonjog

Azokban a joghatóságokban alkalmazandó jogszabályoknak és hatósági előírásoknak való megfelelés érdekében, ahol a Citi üzleti tevékenységet folytat, a Beszállítók a Citi kérésére kötelesek megadni tulajdonosaik adatait – legyenek azok természetes vagy jogi személyek –, ideértve a Beszállító közvetlen tulajdonosát vagy tulajdonosait, egészen a végső tényleges tulajdonosig, aki közvetlenül vagy közvetve, tulajdonjog, ellenőrzés, befolyás vagy más módon rendelkezik irányítással az adott megbízás, termék vagy szolgáltatás felett.

8 CSALÁSOK KEZELÉSE

A Citi csalásokkal kapcsolatos kockázatok azonosítására és enyhítésére irányuló erőfeszítéseinek tekintetében („Csaláskezelés”).

8.1 Minden Beszállító köteles:

1. A törvény által megengedett mértékben együttműködni a Citivel minden feltételezett vagy állítólagos lopás, csalás vagy más potenciális bűncselekmény vagy jogsértés kivizsgálásában, illetve a csalárd tevékenység vagy bűncselekmény miatt indított büntetőeljárásokban;
2. Biztosítani bármely potenciális csalás Citi felé történő időszerű bejelentését és felterjesztését az [Ethics Hotline](#) keresztül. Ide tartozik többek között a megkísérelt, gyanított, állítólagos vagy tényleges lopás, csalás (pl. a Beszállítóval kapcsolatos tudatosan hamisított, pontatlan vagy valótlan adatok benyújtása, számlázási trükkök, pénzeszközök vagy értékpapírok eltűnése stb.), valamint a Citit, a Citi egy alkalmazottját, Beszállítóját, ügynökét vagy egy nem Citi alkalmazottat (pl. ideiglenes munkavállalót vagy alvállalkozót) érintő bűncselekmény vagy szabályszegés;
3. Lehetővé tenni a Citi és a Citi képviselői által végzett megfigyelést és felügyeletet, és támogatni a Beszállítóval kapcsolatos potenciális csalárd tevékenységek Citi – és a hatóságok – által vezetett kivizsgálását;
4. Időben jelenteni minden olyan összeférhetetlenséget (beleértve a Beszállítók/Beszállítói Alkalmazottak és/vagy a Citi Alkalmazottak közötti összeférhetetlenségeket), amelyről a Beszállító tudomást szerez; és
5. Támogatni a Citi csalásmegelőzési folyamatait a Beszállító bankszámlájának a Citi beszállítói fizetési rendszerében való beállítása és frissítése során.

8.2 Továbbá a csalás kockázatának jellegüknél fogva jobban kitett szolgáltatásokat nyújtó Beszállítók **kötelesek**:

1. Dokumentálni és követni egy olyan Csalásellenes kockázatkezelési programot, amely azonosítja a Citinek nyújtott szolgáltatásokhoz kapcsolódó lényeges csalással kapcsolatos kockázatokat, valamint az e kockázatok mérséklésére alkalmazott ellenőrzéseket és eljárásokat.
2. Csalással kapcsolatos tudatosságnövelő képzést tartani (a felvételt követő 90 naptári napon belül, majd ezt követően évente), és az alkalmazottaknak a Citinek nyújtott konkrét szolgáltatásokhoz kapcsolódó csaláskockázati tényezőkre vonatkozó képzést biztosítani.
3. Figyelemmel kísérni a csalási kísérleteket, hatékony belső ellenőrzéseket működtetni a Citinek nyújtott szolgáltatásokkal összefüggő csalási kockázatok csökkentése érdekében, dokumentálni az ellenőrzésekre vonatkozó eljárásokat, folyamatosan vizsgálni azok hatékonyságát, valamint minden feltárt hiányosságot jelenteni az üzleti tevékenységért felelős személynek (BAO).

4. Biztosítani minden szükséges információt az üzleti tevékenységért felelős személynek (BAO) a csalás kockázatának való kitettség folyamatos átvilágításához/figyeléséhez/értékeléséhez.
5. Az átvilágítás keretében Harmadik felekkel kapcsolatos csaláskockázat-értékelési sablont („TP-FIAT”) biztosítani, amelynek célja a Beszállítók csaláskockázat mérséklésére való képességének felügyeleti jellegű értékelése. Ez a működési eljárás azokat a lépéseket írja le, amelyeket az üzleti tevékenységért felelős személy (BAO) vagy a harmadik félként eljáró tisztviselő (TPO) és a csaláskockázat-kezelési tisztviselő (FRMO) hajt végre a csalás kockázatának azonosítása és kezelése érdekében.

8.3 A csalás szolgáltatás jellegéből fakadóan magasabb kockázatát viselő Beszállítók közé egyebek mellett azok tartoznak, akik:

1. hozzáférhetnek olyan Bizalmas vagy magasabb besorolású adatokhoz (ha azok nem a Citi közvetlen ellenőrzése vagy felügyelete alatt állnak), melyekkel csalás válhat lehetővé; ilyenek például a belső számlákhoz, pénzügyi tranzakciókhoz, és készpénzes tranzakciókhoz való hozzáférés.
2. a Citi hálózataihoz/rendszereihez való kapcsolattal rendelkeznek; és
3. olyan szolgáltatásokat és képességeket nyújtanak, támogatnak vagy érnek el, amelyeket csalás elkövetésére vagy annak lehetővé tételére megcélozhatnak, beleértve a következőket:
 - a) Új ügyfelek azonosítása, felvétele vagy jelentkezéseinek feldolgozása;
 - b) Citi- vagy Ügyfélfizetési/Pénzutasítási tevékenységek és/vagy a Citi ügyfeleinek ezen szolgáltatások elérésére való hitelesítése;
 - c) A Citi adatainak vagy a Citi-ügyfelek (pl. demográfiai) adatainak módosítása, a módosítások ellenőrzése vagy végrehajtása;
 - d) Tranzakciós eszközök (pl. bankkártyák/hitelkártyák, elektronikus pénztárcák, csekk-könyvek stb.) biztosítása, gondozása vagy engedélyezése;
 - e) Operatív csaláskezelési tevékenységek végrehajtása vagy támogatása a Citi számára, a csalási események megelőzésével, felderítésével vagy azokra való reagálással kapcsolatban;
 - f) Készpénzhez, pénzügyi eszközökhöz és vagyontárgyakhoz/fizikai árukhoz való fizikai hozzáférés biztosítása;
 - g) Kísérő nélküli vagy munkaidőn kívüli hozzáférés a Citi létesítményeihez;
 - h) Pénzügyi kimutatások: számviteli tevékenységek, például tételek rögzítése a főkönyvben/analitikai nyilvántartásban;
 - i) Támogatott tevékenységekért járó jutalmak szerzése és elköltése.

9 MÉDIA KERETEIN BELÜLI INTERAKCIÓK ÉS NYILVÁNOS MEGJELENÉSEK

A Citi vállalati szolgáltatásokért, valamint globális közügyekért felelős osztálya az egyetlen, amelynek jogában áll sajtóközleményeket kiadni vagy nyilvánosan felszólalni a

Citi nevében. A Beszállítók nem adhatnak ki olyan sajtóközleményt, amely közvetlenül vagy közvetve azonosítja a Citit, a Beszállító és a Citi közötti Szerződéseket vagy megállapodásokat vagy a Citi által a Beszállítótól beszerzett termékeket és szolgáltatásokat. A Beszállítók nem járulhatnak hozzá és nem vehetnek részt Citihez fűződő közönségkapcsolati tevékenységekben az ügyfelekkel, a Citi alkalmazottjaival, a Citi más Beszállítóival, a Beszállítók más ügyfeivel vagy más harmadik felekkel az elsődleges Citi üzleti kapcsolattartó előzetes írott jóváhagyása nélkül.

A Beszállítók elsődleges Citi üzleti kapcsolattartójuk és az országos közönségkapcsolati vezető előzetes írásbeli jóváhagyása nélkül nem jogosultak közzétenni vagy nyilvánosságra hozni semmilyen írásos vagy elektronikus formátumú anyagot (beleértve a könyveket, cikkeket, podcastokat, webcastokat, blogokat, weboldalakon közzétett tartalmakat, fényképeket, videókat, közösségi médiát vagy egyéb médiaanyagokat), amely a Citit, a Citi működését, Ügyfeleit, termékeit vagy szolgáltatásait említi, illetve nem tarthatnak beszédeket, nem adhatnak interjúkat, és nem léphetnek fel nyilvánosan ilyen anyagokkal.

A Citi előzetes írott jóváhagyása nélkül a Beszállítók nem használhatják a Citi tulajdonosi ismertetőjegyeit, védjegyeit, szolgáltatási jegyeit, kereskedelmi neveit, emblémáit, szimbólumait vagy márkaneveit, sem a szolgáltatások vagy termékek Citi számára történő biztosításával kapcsolatban, sem attól függetlenül. A Beszállítók nem használhatják fel a Citi nevét, logóját vagy védjegyeit, létesítményeit vagy kapcsolatait előnyökre vagy a Citin kívüli munkára (beleértve a fejléces vagy személyes webhelyeket, blogokat vagy más közösségi oldalakat). Ezenkívül a Beszállítók nem használhatják fel a Citi nevét, létesítményeit vagy kapcsolatait jótékonyági vagy pro bono célokra.

10 ELEKTRONIKUS ÍRÁSBELI KOMMUNIKÁCIÓ

Amikor a Citi személyzetével kapcsolatba lépnek, vagy a Citi számára vagy nevében teljesítik kötelezettségeiket, a Beszállítók kizárólag a Citi által jóváhagyott írásbeli Elektronikus kommunikációs eszközöket, rendszereket és szolgáltatásokat használhatják. A Citivel való kapcsolattartásra használt új vagy átdolgozott elektronikus kommunikációs csatornákat, legyenek akár önálló eszközök, akár egy tágabb platformba beépítettek, a Citi vagy harmadik fél által biztosítottak, jóvá kell hagyni a vonatkozó Citi Követelményeknek megfelelően, amelyekről a BAO előzetesen írásban értesíti a Beszállítót. A Citi által nem jóváhagyott üzenetküldő platformokon, mint amilyen a WhatsApp, a WeChat, a LINE, a Slack, a Signal, a Telegram, az iMessage, az SMS, a Viber, valamint bármilyen egyéb interaktív elektronikus platformon tilos a Citi üzleti tevékenységével kapcsolatban a Citi személyzetével kommunikálni.

Ezenfelül a Beszállítók nem támaszthatnak titoktartással kapcsolatos elvárásokat a Citi által biztosított Kommunikációs eszközökön, rendszereken és szolgáltatásokon keresztül létrehozott, felfedezett, használt, elért, letöltött, tárolt, továbbított, fogadott vagy törölt írásbeli Elektronikus kommunikációval kapcsolatban. A Citi figyelemmel kísérheti az Elektronikus kommunikációs eszközöket, rendszereket és szolgáltatásokat, valamint

magát az Elektronikus kommunikációt is. Az ilyen Elektronikus kommunikáció a Citi tulajdonát képezi, és a nyilvántartások megőrzésére vonatkozó követelményeknek megfelelően megőrizhető (a helyi törvények és szabályozások függvényében).

<https://policydirectory.citi.net/cpd/ layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 POLITIKAI TEVÉKENYSÉGEK ÉS HOZZÁJÁRULÁSOK

Különbéle jogszabályok – többek között az alábbi területekre vonatkozók – szabályozzák: külföldi befolyásolás; kampányfinanszírozás; ajándékok és vendéglátás; jogalkotási, társadalmi, bizalomépítő- és szabályozási lobbitevékenység; beszerzés; pay-to-play gyakorlatok; valamint értékpapírok. E jogszabályok a Citi és Beszállítói politikai tevékenységére, valamint az ilyen tevékenységekkel kapcsolatos közzétételi kötelezettségekre vonatkoznak. A Beszállítók kötelesek tartózkodni minden olyan politikai tevékenységtől, mely nem felel meg a Citi vonatkozó irányelveinek és szabványainak, illetve a vonatkozó törvényeknek vagy szabályozásoknak.

A politikai tevékenység például, a teljesség igénye nélkül:

1. Vállalati vagy személyes politikai hozzájárulások, politikai hozzájárulások igénylése, a vállalat tőkéjének vagy erőforrásainak (pl. létesítményeinek, berendezéseinek, szoftvereinek vagy személyzetének) felhasználása vagy a vállalatnál töltött idő alatt teljesített személyes szolgáltatások önkéntes felajánlása egy politikai pozíció betöltésére jelölt személynek, egy politikai párt bizottságának vagy egy politikai bizottságnak;
2. Köztisztviselőknél való lobbizás vagy azok bármilyen más formájú, közvetlen vagy harmadik feleken keresztül megkeresése, ideértve többek között a tisztviselők vagy a törvényhozás befolyásolására irányuló kísérleteket és – a joghatóság függvényében – akár az ügynökségi szabályozás vagy az állami szerződések odaítélésének befolyásolására irányuló kísérleteket is; és
3. Kormányzati kötődésű politikai pozícióra való pályázás, vagy ilyen pozíció elfogadása vagy betöltése, beleértve a kormánybizottságokon, -testületeken vagy más hasonló szervezeteken belüli pozíciókat.

A Beszállítók semmilyen politikai tevékenységet nem végezhetnek a Citi vagy ügyfelei nevében (vagy állítólagosan nevében) a Citi Kormányzati ügyekért felelős globális műveleti ellenőrzési osztályának (ggacontrol@citi.com) előzetes írásbeli engedélye nélkül. Bár a Citi adott esetben díjat és/vagy költségtérítést fizet a Beszállító által nyújtott szerződéses és megengedett politikai tevékenységekkel kapcsolatos szolgáltatásokért, például a lobbitevékenységért, a Citi soha nem téríti meg a Beszállító vagy alkalmazottai által tett személyes vagy vállalati politikai hozzájárulásokat.

12 PÉNZMOSÁS-ELLENESSÉG („AML”)

Azokra a Beszállítókra vonatkozik, amelyek bizonyos ügyfélkapcsolati szolgáltatásokat nyújtanak (pl. ügyfélbeléptetés, ügyfélszámlák és tranzakciók átvilágítása), illetve az ezekhez kapcsolódó adatokat vagy mutatókat szolgáltatják; ÉS/VAGY pénzügyi tranzakciók vagy pénzügyi eszközök tekintetében közvetítőként járnak el (pl. távoli csekkbefizetés-feldolgozás, futárszolgálat, pénzszállító szolgáltatás, lockbox szolgáltatás, elektronikus átutalások vagy digitális eszközök kezelése).

12.1 Pénzmosás elleni (AML) kötelezettségek:

1. A Citi folyamatai és az Alkalmazandó Jogszabályok betartása:

- Fenn kell tartani és követni kell a Citi azon folyamatait és eljárásait, melyek a vonatkozó jogszabályok követelményeinek való megfelelésre lettek kialakítva; ilyen jogszabályok (i) a Gramm-Leach-Bliley törvény és az az alapján kihirdetett rendeletek; (ii) az USA PATRIOT törvény és az az alapján kihirdetett rendeletek; (iii) bármilyen pénzmosással foglalkozó törvény vagy rendelet; és (iv) bármilyen gazdasági szankciókkal kapcsolatos törvény vagy rendelet. E szabályzatoknak és eljárásoknak ki kell térniük a pénzmosás elleni feladat- és felelősségi körökre, beleértve azt a követelményt is, hogy a pénzügyi tevékenységekkel, tranzakciókkal vagy készpénzbefizetésekkel kapcsolatos minden szokatlan vagy potenciálisan szokatlan tevékenységet haladéktalanul jelenteni kell.

2. A Személyzet részére biztosítandó éves képzés és a program elemei:

- A Beszállító köteles biztosítani, hogy a Citinek Szolgáltatásokat nyújtó Személyzet évente pénzmosás elleni képzésben részesüljön, amely kiterjed a pénzmosás elleni feladat- és felelősségi körökre, valamint arra a kötelezettségre, hogy a pénzügyi tevékenységekkel, tranzakciókkal vagy készpénzbefizetésekkel összefüggő minden szokatlan vagy potenciálisan szokatlan eseményt haladéktalanul jelenteni kell. A képzésnek legalább az alábbi témaköröket kell magában foglalnia:
 - a. A gyanús tevékenységek bejelentése és eskalációja.
 - b. Az „Ismerd meg ügyfeledet” (KYC) program, beleértve az ügyfél-azonosítási (CIP) programot, a szankciós és névellenőrzést, az ügyfél-átvilágítást (CDD), a fokozott ügyfél-átvilágítást (EDD), valamint a **végző tényleges tulajdonosok (UBO-k)** azonosítását és ellenőrzését.
 - c. Tranzakciók nyomon követése valamennyi releváns pénzügyi eszköz és pénzügyi tevékenység tekintetében.

- d. Időszakos jelentések és mérőszámok, beleértve a jogszabályi és szabályozási változásokról, valamint az AML program lényeges módosításairól szóló jelentéseket is.
- e. Az AML program hatékonyságának tesztelése és az ahhoz kapcsolódó belső ellenőrzések működtetése, beleértve a helyszíni ellenőrzéseket is.

3. Szerződéses rendelkezések betartása:

- A Szerződés minden olyan rendelkezésének betartása, amely meghatároz egy a Beszállító által bevezetendő programot.

4. A feltételezett jogsértések haladéktalan bejelentése:

- A Citinek haladéktalanul, írásban be kell jelenteni minden feltételezett jogsértést, beleértve minden olyan szokatlanul vagy potenciálisan szokatlanul tűnő észlelt tevékenységet is, amely készpénzbefizetésekkel, pénzügyi tevékenységekkel, illetve a Citi vagy annak ügyfeleit érintő tranzakciókkal kapcsolatos.

5. Az adóelkerülés megelőzése és bejelentése:

- Az összes vonatkozó adótörvény és -szabályozás betartása a működési országokban.
- A Beszállítók semmilyen körülmények között sem vehetnek részt szándékos illegális adóelkerülésben, és nem segíthetnek elő másokat ilyen adóelkerülésben, beleértve az olyan tevékenységeket is, amelyek elősegítik az esedékes és fizetendő adók megfizetésének elkerülését, vagy információ eltitkolását az adóhatóságok elől.
- Ezáltal észszerű megelőzési eljárásokat kell elfogadniuk az adócsalásokat illetően, és haladéktalanul, írásban jelentést kell tenniük a Citi felé a Citiivel kapcsolatos bármilyen jogsértés vagy vélelmezett jogsértés esetén.

12.2 A Beszállító belső szabályzatai és eljárásai:

A Beszállítók kötelesek megfelelő belső szabályzatokat és eljárásokat fenntartani a jelenleg hatályos vagy a jövőben hatályba lépő összes AML jogszabály és szabályozás betartása érdekében.

13 NYILVÁNTARTÁSOK KEZELÉSE

Azokra a Beszállítókra vonatkozik, akik elérik/feldolgozzák/tárolják a Citi-információkat.

A Citi előírja, hogy minden olyan Beszállító, amely Citi-információkat kezel vagy őriz, működjön együtt a kijelölt üzleti tevékenységért felelős személlyel („BAO”) vagy elsődleges Citi üzleti kapcsolattartójával annak érdekében, hogy (i) a Citi nyilvántartáskezelési céljaira az Információkat azonosítsák és Nyilvántartásként vagy Átmeneti Információként besorolják, (ii) a Nyilvántartásokat a Citi Fő Nyilvántartási Katalógusának („MRC”) megfelelően osztályozzák, (iii) az Információkat a Citi megőrzési követelményeinek megfelelően megőrizték, valamint (iv) Információmegőrzési Rendelkezés hiányában az Információs életciklus végén az Információkat megfelelő módon megsemmisítsék.

Az üzleti tevékenységért felelős személy vagy elsődleges Citi üzleti kapcsolattartó a Beszállítóval együttműködve biztosítja, hogy az a Citi Fő nyilvántartási katalógusában szereplő nyilvántartások kódjai szerint azonosítsa és osztályozza a nyilvántartásokat, a Nyilvántartásjegyzéket legalább évente frissítve. A Beszállító köteles betartani a BAO által közölt Iratkezelési Követelményeket. A selejtezési feltételeknek megfelelő nyilvántartásokat a lehető legrövidebb időn belül, de legkésőbb a megőrzési követelmények teljesülését követő hat hónapon belül megfelelő módon meg kell semmisíteni, kivéve, ha azokra Információmegőrzési Rendelkezés vonatkozik. Az Átmeneti Információkat legkésőbb az utolsó felhasználást követő két éven belül meg kell semmisíteni, kivéve, ha az Információmegőrzési Rendelkezés hatálya alá esnek. A személyes adatokat tartalmazó Átmeneti Információkat haladéktalanul törölni kell, amint az adatgyűjtés célja megvalósult, kivéve, ha azokra az Információmegőrzési Rendelkezés vonatkozik. A Beszállító köteles felfüggeszteni a Citivel kapcsolatos információk megsemmisítését vagy módosítását, ha Információmegőrzési Rendelkezés alkalmazásáról értesítik. A Beszállító bármilyen kétség esetén köteles egyeztetni az elsődleges Citi üzleti kapcsolattartójával vagy a BAO-val.

Az Országos Megőrzési Ütemtervekben felsorolt megőrzési szabályokat a DCRM negyedévente felülvizsgálja és szükség szerint frissíti a szabályozási és belső változásoknak megfelelően. Amennyiben a Beszállítót érintő változás történik, a BAO arról értesítést küld. A Beszállító köteles felmérni a változások hatását, és végrehajtani a szükséges módosításokat az érintett rendszerekben, folyamatokban és nyilvántartásokban. A Beszállító a BAO értesítésétől számított 90 napon belül köteles végrehajtani a szükséges módosításokat az általa kezelt és tulajdonolt nyilvántartástípusok tekintetében.

A Citi nevében dokumentumokat kezelő Beszállítók felelősek minden olyan Információ megőrzéséért („tárolásáért”), gyűjtéséért és előállításáért, amelyet jogi vagy egyéb eljárás szempontjából relevánsnak ítélnék, a BAO által kért határidőt figyelembe véve. A Beszállító köteles a Citi kérésére a vonatkozó szerződéses rendelkezéseknek megfelelően visszaszolgáltatni a Citi információit. A Beszállítók elsődleges Citi üzleti

kapcsolattartójuk vagy a BAO jóváhagyása nélkül nem jogosultak megsemmisíteni semmilyen Citi-információt, függetlenül annak besorolásától (pl. bizalmas, nem bizalmas); az esetleges jóváhagyásnak meg kell erősítenie, hogy a megsemmisítendő információkra nem vonatkozik aktív Információmegőrzési Rendelkezés. A nyilvántartáskezelési és -megőrzési követelmények, valamint az egyéb információkezelési követelmények hatályban maradnak a Szerződés megszűnését vagy lejártát követően is, kivéve, ha a Felek kifejezetten másként állapodnak meg.

A Beszállítók kötelesek dokumentációt vezetni, melyben felsorolják a beszállítói Személyzet összes olyan tagját, aki a Beszállító illetékességébe eső Citi-információ kezelésének felügyeletéért felelős, és kötelesek rendszeres időközönként megbeszéléseket tartani elsődleges Citi üzleti kapcsolattartójukkal vagy Nyilvántartáskezelési tisztviselőjükkel, hogy felülvizsgálják és áttekintsék a kapcsolattartók neveit, az eljárási részleteket, a szerep- és felelősségköröket, valamint a Citi beszállítói Nyilvántartásjegyzékét.

14 VÁLLALATI RUGALMASSÁG/ÜZLETMENET-FOLYTONOSSÁG

Azokra a Beszállítókra vonatkozik, akik a Citi által használt szolgáltatásokat nyújtanak, vagy ilyen technikai jellegű infrastruktúrát/alkalmazásokat üzemeltetnek. A Citi által kijelölt üzleti tevékenységért felelős személy (BAO) felelőssége tájékoztatni a Beszállítót az alkalmazhatóságról és az üzletfolytonossági követelményekről.

14.1 Helyreállítási erőforrások

A Beszállítók katasztrófa-helyreállítási tervének olyan alternatív erőforrásokat kell biztosítania, melyek megfelelőek arra, hogy az összes terméket és szolgáltatást eljuttassák a Citi számára, ha a Beszállító elsődleges telephelye elérhetetlenné válna. A helyreállítási erőforrásoknak az elsődleges helyszínektől földrajzilag eltérő helyen kell lenniük, elegendő távolságra ahhoz, hogy minimalizálható vagy kiküszöbölhető legyen annak a veszélye, hogy ugyanaz a katasztrófa az elsődleges és a helyreállítási helyszíneket is érintse.

1. A helyreállítási erőforrások nem korlátozódnak az információs rendszerekre, hanem magukban foglalják a termékek és szolgáltatások Citi számára történő folyamatos biztosításához szükséges összes erőforrást is, amely kiterjedhet a személyzetre, épületekre, üzleti berendezésekre, adatközpontokra, adat- és hálózati hálózatokra, valamint a szállítási szolgáltatásokra.
2. Az alkalmazást biztosító Beszállítók a Magas rendelkezésre állású konfiguráció biztosításának érdekében alkalmazhatnak két aktív, párhuzamosan működő rendszerarchitektúrát. Ez az elrendezés megköveteli, hogy (legalább) két azonosan konfigurált rendszer működjön és legyen elérhető az ügyfelek/felhasználók számára. A modell legfontosabb funkciója, hogy az alternatív környezet(ek) egyidejűleg fut(nak) az elsődleges (fő) adatközponttal.

14.2 Helyreállítási szolgáltatási szintek

A Beszállítók üzletmenet-folytonossági terveinek meg kell felelniük bizonyos szolgáltatási szinteknek ahhoz, hogy a Citi szempontjából hatékonyak legyenek. A Beszállító katasztrófa-helyreállítási tervének konkrét értékeket kell meghatároznia legalább a következőkre vonatkozóan:

1. Célzott helyreállítási idő
2. Helyreállítási pontra vonatkozó célkitűzés
3. Helyreállítási erőforrások / technológiai kapacitás
4. Helyreállítási időtartam

14.3 Katasztrófa-helyreállítási terv

A Beszállító köteles katasztrófa-helyreállítási tervet fenntartani az üzletmenet folytonossága érdekében (és ennek aktuális és időszakos teszteléséről igazolást kell biztosítania a Citi kérésére), hogy a Beszállító a Termékeknek/Szolgáltatásoknak vagy az alábbi egyéb kötelezettségeinek egy adott helyről vagy adott személyek erőfeszítései révén történő biztosításában, illetve teljesítésében bekövetkezett zavar esetén is haladéktalanul képes legyen a Termékek/Szolgáltatások biztosítására és a kötelezettségei teljesítésére egy másik helyről vagy helyettesítő Személyzet révén. A katasztrófa-helyreállítási terv egy példányát a Citi rendelkezésére kell bocsátani a Citi és a Beszállító között létrejött egyes Munkarendelések hatálybalépésének napjától számított 10 (tíz) naptári napon belül, majd ezt követően évente, mindaddig, amíg az egyes Munkarendelések hatályban maradnak. A Beszállító a katasztrófa-helyreállítási tervben köteles olyan utasításokat és információkat meghatározni, melyek biztosítják, hogy a Citi továbbra is igénybe tudja venni a Termékeket/Szolgáltatásokat, akkor is, ha a Beszállítónak életbe kellett léptetnie a katasztrófa-helyreállítási tervet. A Beszállító ezúton kijelenti, szavatolja és kötelezettséget vállal arra, hogy a katasztrófa-helyreállítási terve tartalmazza legalább a következőket:

1. Azokat a helyreállítási eljárásokat és stratégiákat, beleértve az áthelyezést, a munka átirányítását és/vagy a távoli hozzáférést, amelyek a zavarok hatásának enyhítését célozzák; ilyen zavarok például az elérhetetlenné vált technológia (szolgáltatásmegtagadás/DoS), az elérhetetlenné vált elsődleges munkahelyszín (hozzáférés megtagadása/DoA), valamint az elérhetetlenné vált személyzet (beleértve az alvállalkozókat is);
2. A Beszállító által biztosított karbantartást, amely kiterjed (többek között, de nem kizárólagosan) egy, a Termék/Szolgáltatás helyszíneitől elkülönített másodlagos katasztrófa-helyreállítási telephelyre; biztonsági mentésre szolgáló adathordozók tárolását a Termék/Szolgáltatás helyszíneitől elkülönített helyen; redundáns kommunikációs vonalak és szerverek használatát stb.;
3. A Termékek/Szolgáltatások működésének és alkalmazásának biztonsági mentésére/helyreállítására vonatkozó eljárásokat, beleértve egy részletes, dokumentált tervet a Termékekben/Szolgáltatásokban áramkimaradás, rendszerhiba, természeti katasztrófa vagy egyéb előre nem látható körülmény következtében bekövetkező zavarra való

- reagáláshoz, amely magában foglalja a működés közösen megállapított időtartamon belüli folytatásához szükséges folyamatokat és eljárásokat;
4. Az összes Tartalom védelmére szolgáló eljárásokat;
 5. A helyettesítő eszközökre (pl. számítástechnikai berendezésekre) vonatkozó eljárásokat, valamint az ezek biztosítását szabályozó harmadik felekkel kötött megállapodásokat;
 6. A telephelyen kívüli gyártólétesítményekre vonatkozó eljárásokat; valamint
 7. A Beszállító katasztrófa-helyreállítási terve biztosítja a következőket:
 - a. A Beszállító haladéktalanul értesíti a Citi minden olyan katasztrófáról, amely negatív hatással lehet a Termékekre/Szolgáltatásokra;
 - b. A Beszállító az értesítéstől számított 24 órán belül tervet nyújt be a Citi számára a Termékek/Szolgáltatások másik feldolgozó létesítményben történő folytatására vonatkozóan;
 - c. A Termékeknek/Szolgáltatásoknak teljes mértékben működőképesnek kell lenniük az előírt Helyreállítási időcélon (RTO) belül, amely – ha a vonatkozó szerződés másként nem határoz – a Citi által „Üzleti szempontból kritikus”- vagy „MAGAS” fontossági besorolással ellátott folyamatoknál legfeljebb 4 óra, a Citi által „KÖZEPES” fontossági besorolással ellátott folyamatoknál legfeljebb 24 óra, a Citi által „ALACSONY” fontossági besorolással ellátott folyamatoknál pedig legfeljebb 72 óra; valamint
 - d. Amennyiben a Beszállító létesítményeinek egyes részei működésképtelenné válnak, a Beszállító nem bánhat a Citiivel kedvezőtlenebbül, mint más kereskedelmi ügyfeleivel.

14.4 A Hosztolt szolgáltatásokra vonatkozó katasztrófa-helyreállítási terv követelményei

Amennyiben a Beszállító Hosztolt szolgáltatást kezel és biztosít a Citi számára, a következő rendelkezések is alkalmazandók. A katasztrófa-helyreállítási tervnek tartalmaznia kell legalább a következőket:

1. A hosztolt szolgáltatások működésének és alkalmazásának biztonsági mentésére/helyreállítására vonatkozó eljárásokat, beleértve egy részletes, dokumentált tervet a Szolgáltatásokban áramkimaradás, rendszerhiba, természeti katasztrófa vagy egyéb előre nem látható körülmények következtében bekövetkező zavarra való reagáláshoz, amely magában foglalja a működés közösen megállapított időtartamon belüli folytatásához szükséges folyamatokat és eljárásokat;
2. A Beszállító katasztrófa-helyreállítási tervének a következőket is biztosítania kell: (a) a Beszállító két (2) órán belül írásban értesíti a Citi minden olyan katasztrófáról, amely negatívan érintheti a Hosztolt Szolgáltatásokat; (b) a Beszállító az értesítéstől számított 24 órán belül tervet nyújt be a Citi számára a Hosztolt Szolgáltatások másik feldolgozó

létesítményben történő folytatására vonatkozóan, valamint (c) a Hosztolt Szolgáltatásoknak az első értesítéstől számított 48 órán belül teljesen működőképesnek kell lenniük;

3. A Beszállító vállalja, hogy kérésre kiad minden információt, melyre a Citi katasztrófa-helyreállítási tervének és üzletmenet-folytonossági tervének kidolgozásához szükség van, hogy az a Beszállító katasztrófa-helyreállítási tervével és üzletmenet-folytonossági tervével összhangban működhessen; és
4. Amennyiben a Beszállító létesítményeinek egyes részei működésképtelenné válnak, a Beszállító nem bánhat a Cítivel kedvezőtlenebbül, mint más kereskedelmi ügyfeleivel.

14.5 A katasztrófa-helyreállítási terv módosításai

A Beszállító jogosult módosítani a Katasztrófa-helyreállítási tervét, amennyiben a változtatások nem rontják a Katasztrófa-helyreállítási terv minőségét, illetve várhatóan nem befolyásolják hátrányosan a szolgáltatásokat (pl. nem hosszabbítják meg a Helyreállítási időcélakat). A Beszállító köteles haladéktalanul értesíteni Citi-t a Katasztrófa-helyreállítási tervében bekövetkezett bármilyen módosításról, és kérésre magyarázatokat ad, hogy a Citi teljes mértékben megértse azokat és reagálni tudjon.

14.6 Alvállalkozók katasztrófa-helyreállítási terve

A Beszállító köteles biztosítani, hogy valamennyi alvállalkozója a Citi Beszállítói Követelményeivel összhangban álló katasztrófa-helyreállítási tervet és kapcsolódó üzletmenet-folytonossági kontrollokat tartson fenn. A Beszállító köteles megfelelő felügyeletet gyakorolni alvállalkozói felett, ideértve a kontrollok és a teszteredmények rendszeres felülvizsgálatát, valamint biztosítani az azonosított hiányosságok időben történő megszüntetését.

14.7 Katasztrófa-helyreállítási terv alkalmazása és vészhelyzetről való értesítés

A Beszállítók kötelesek haladéktalanul értesíteni az elsődleges Citi üzleti kapcsolattartójukat:

1. Ha a Beszállító életbe lépteti a katasztrófa-helyreállítási tervét; és
2. Minden olyan, a Beszállítót vagy annak Alvállalkozóit érő válságról, fenyegetésről, figyelmeztetésről vagy kiberbűnözési eseményről, amelyről észszerűen feltételezhető, hogy káros hatással van a Citi részére nyújtott Szolgáltatásokra vagy Termékekre.

14.8 Tesztelés

A Beszállító köteles tesztelni összes helyreállítási erőforrását és tervét a termelési bevezetést követő 120 napon belül (a Citi által vállalati szempontból kritikusnak minősített alkalmazások esetén 90 napon belül), majd legalább évente (12 havonta). A tesztelésnek igazolnia kell, hogy a Beszállító a Citi számára biztosított összes termék és szolgáltatás esetében képes elérni a helyreállítási szolgáltatási szinteket. Ezeknek a teszteknek átfogónak kell lenniük, és ki kell terjedniük a Citi számára nyújtott Szolgáltatások teljes körére. A Beszállító köteles legalább 30 naptári napos előzetes értesítést küldeni a Citi-nek a számára biztosított termékeket/szolgáltatásokat érintő helyreállítási tesztekéről. A Citi jogosult részt venni a Beszállító helyreállítási

tesztelésében vagy megfigyelni azt, hogy a Citi által használt alkalmazások üzleti funkcionalitását a helyreállítási környezetben validálja. Amennyiben a Citi részt kíván venni a tesztelésben, a Beszállító a teszt elvégzése előtt köteles megosztani a Citivel a teszt célkitűzéseit, a tesztelési tervet és a teszthelyszínhez való csatlakozásra irányuló eljárásokat. A Beszállító az egyes tesztek elvégzését követő tíz (10) munkanapon belül köteles átadni a Citinek a tesztelés célkitűzéseinek összefoglalóját, a tesztre vonatkozó tervet, valamint a teszteredményeket, beleértve a helyreállításhoz szükséges időkereteket és a teszteredményeket igazoló bizonyítékokat (pl. képernyőképeket).

14.9 Mennyiség érvényesítése

A Citi által vállalati szempontból kritikusnak minősített alkalmazásokat üzemeltető Beszállítók kötelesek igazolni, hogy a Termelési mennyiségek feldolgozhatók üzletmenet-folytonossági/katasztrófa-helyreállítási környezetében. A Citinek és Beszállítónak a validációra alkalmazandó módszertanban közösen kell megállapodniuk.

14.10 A Citi rendszereinek szolgáltatások nyújtására való használata

Amennyiben a Citi vagy a Citi leányvállalatai kérelmezik, a Citi rendszereit használó Beszállítók kötelesek a Citi számára díjmentesen részt venni a Citi katasztrófa-helyreállítási gyakorlataiban.

14.11 A teszteredmények kezelése

Amennyiben a Beszállító által végzett tesztelés bármely eredménye azt mutatja, hogy nem sikerült teljesíteni a teszt célkitűzéseit vagy bármely vonatkozó helyreállítási idő célt, úgy a Beszállító köteles feltárni az eredendő okot, és haladéktalanul orvosolni az azonosított hiányosságokat. A helyzet orvoslását követően a Beszállító köteles ismételt tesztet végezni az első megghiúsult tesztől számított legfeljebb százhusz (120) naptári napon (a Citi által vállalati szempontból kritikusnak minősített alkalmazások esetén 90 napon belül) belül (vagy a vonatkozó Munkarendelésben megadott időszakon belül).

14.12 Kríziskezelés

Az üzletmenet-folytonossági tervvel összefüggésben a Beszállító köteles válságkezelési tervet fenntartani a helyreállítási műveletek irányítására és ellenőrzésére. A Beszállító válságkezelési tervének meg kell határoznia legalább a helyreállítási művelet elindításához megfelelő jogosultsággal rendelkező személyeket, meg kell határoznia a kommunikációs és eskalációs protokollokat a válságra vonatkozó információk összegyűjtésére és terjesztésére, valamint tartalmaznia kell azokat az értesítési és eskalációs protokollokat, amelyek a Citivel való kommunikációra vonatkoznak válság esetén.

14.13 Üzletmenet-folytonossági értékelések

A Beszállítókra nézve kötelező érvényű a Citi harmadik felekre vonatkozó üzletmenet-folytonosság-kiértékelési folyamata, amelynek során kiértékelik, hogy a Beszállító szabályzatai, eljárásai és ellenőrzésre szolgáló eszközei mennyire felelnek meg a Citi követelményeinek, valamint az üzletmenet-folytonosságra vonatkozó (a Citivel vagy a Beszállítóval szembeni) jogi és/vagy szabályozási követelményeknek. Az értékelés olyan kérdőívekből áll, amelyeket a Beszállítónak alátámasztó bizonyítékokkal együtt kell megválaszolnia, és kiterjedhet a Beszállító telephelyeire való látogatásra is. Ha az értékelés problémákat vagy aggályokat fed fel vagy jelez, akkor a Citi dokumentálja az

eredményeket, és a Beszállítóval együttműködve megpróbálja megállapítani, hogyan lehet kiküszöbölni a problémákat. A Beszállítók kötelesek haladéktalanul elvégezni a szükséges korrekciókat, és/vagy bevezetni a szükséges kompenzáló ellenőrzéseket az aggályok a Citi számára elfogadható mértékű kezelésére.

14.14 Működési rugalmasság

A kritikus üzleti szolgáltatások azok a szolgáltatások, amelyek biztosításának megszakadása jelentős káros hatást gyakorolhat a Citire, a Citi ügyfeleire vagy a pénzügyi rendszerre. A Beszállítónak gondoskodnia kell arról, hogy a szolgáltatások azon elemeinek nyújtásában bekövetkező zavarok, amelyek vagy kritikus üzleti szolgáltatásoknak minősülnek, vagy a kritikus üzleti szolgáltatások Citi általi nyújtását támogatják, a Citi által időről időre meghatározottak szerint („Kritikus üzleti szolgáltatások”) ne haladják meg a Citi által meghatározott időtartamot, illetve ne sértsék meg más módon a Citi által meghatározott mérőszámokat („Hatástűrések”), amelyekről időről időre értesíti a Beszállítót. A Hatástűrések egyértelmű, időtartamhoz kötött mérőszámként kerülnek meghatározásra, amely azt az időtartamot fejezi ki, ameddig a szolgáltatásnyújtás megszakadhat. A Citi és a Beszállító évente felülvizsgálják a Hatástűréseket a folyamatban lévő szerződésirányítási folyamat keretében. Ha a Citinek egynél több szabályozó testület követelményei miatt egynél több Hatástűrést kell meghatároznia egy adott Kritikus üzleti szolgáltatáshoz, akkor a Citi különálló Hatástűréseket határozhat meg az érintett Kritikus üzleti szolgáltatásokhoz. A Beszállító köteles:

1. Értesíteni a Citit, amint tudomást szerez arról, hogy elmulasztotta (vagy észszerű alapon valószínű, hogy el fogja mulasztani) valamely szolgáltatás a Citi által meghatározott megfelelő Hatástűrés(ek) értékein belüli teljesítését, az esetleges vagy tényleges meghibásodás indokaival kapcsolatos magyarázatot, illetve a mulasztás hatásának enyhítésére tett lépéseket is leírva;
 2. Kérésre észszerű segítséget nyújtani a Citinek, hogy képes legyen azonosítani azokat az embereket, folyamatokat, technológiákat, létesítményeket és információkat, amelyekre a Beszállítónak szüksége van valamely Kritikus üzleti szolgáltatás nyújtásához;
 3. Észszerű segítséget nyújtani a Citinek, hogy az végrehajthassa a következőket:
 - a. bármilyen belső forgatókönyv-tesztelés elvégzését arra vonatkozóan, hogy a Beszállító képes-e az egyes kritikus üzleti szolgáltatásokra vonatkozó hatástűrés(ek)en belül maradni, ha súlyos, de valószínűsíthető zavar lép fel a saját vagy a Beszállító működésében; és
 - b. a forgatókönyv-tesztelést követően a tanulságok levonását, lehetővé téve a Citi számára a gyengeségek, valamint a Beszállító jövőbeli zavarokra való hatékony reagálási és helyreállítási képességének javításához szükséges intézkedések azonosítását.
- Ha a Citi által végzett belső forgatókönyv-tesztelés sebezhetőséget vagy korlátokat azonosít a Beszállító azon képessége kapcsán, hogy szolgáltatásokat nyújtson a Citi által meghatározott megfelelő

Hatástűrés(ek) értékein belül, valamint azt követően, hogy a Beszállító mulasztást követ el bármely szolgáltatás a Citi által meghatározott megfelelő Hatástűrés(ek) értékein belüli biztosításának tekintetében, a felek megállapodnak egy tervről (beleértve a terv végrehajtásának ütemezését is), biztosítva, hogy a Beszállító megtegye a szükséges lépéseket az adott sebezhetőségek vagy korlátozások megszüntetésére vagy enyhítésére, illetve a Hatástűrés(ek) értékeinek meghaladását kiváltó ok orvoslására, az észszerűen lehetséges legrövidebb időn belül.

14.15 Letéti megállapodás

A Citi kérésére azok a Beszállítók, (i) akik szoftvert engedélyeztetnek a Citinek Citi-környezetben való működéshez, vagy (ii) akik Hosztolt szolgáltatást nyújtanak a Citinek, kötelesek biztosítani, hogy a Letétbe helyezett anyagokat a Citi kijelölt letéti ügynökénél helyezték letétbe, és aláírják a vonatkozó letéti szerződés értelmében Letétbe helyezett anyagokra vonatkozó letéti regisztrációs jegyzéket vagy a letéti ügynök által előírt egyéb nyomtatványokat. Ezt követően a licencekre vagy a Hosztolt szolgáltatásra vonatkozó megállapodás fennmaradó időtartama alatt a Beszállító letétbe helyezi a letéti ügynöknel a Letétbe helyezett anyagok frissített verzióit, hogy a letétbe helyezett Forráskód és egyéb Letétbe helyezett anyagok mindig naprakészek legyenek, a Citi által használt szoftver- vagy Hosztolt szolgáltatás szoftverének legújabb verziójával. A Forráskód és egyéb Letétbe helyezett anyagok frissítéseit kézbesíteni kell a letéti ügynöknek a Citinek engedélyezett szoftver frissítésének vagy a Citi által használt Hosztolt szolgáltatások módosításának dátumától számított harminc (30) napon belül. A Beszállító köteles maradéktalanul betartani a letéti szerződés által a letétesnek előírt kötelezettségeket és követelményeket. A Beszállító köteles kizárólagosan viselni minden letéti költséget és díjat, beleértve, a teljesség igénye nélkül, a kezdeti költségeket, az éves díjakat, a betéti díjakat, a szolgáltatási díjakat és minden egyéb letéti díjat és költséget. Megszűnési esemény esetén a Letéti ügynök a Letétbe helyezett anyagokat a Citinek vagy a Citi által kijelölt képviselőnek adja át, az alapul szolgáló megállapodás és a letéti szerződés feltételeinek megfelelően.

Amennyiben a Forráskód (vagy más Letétbe helyezett anyag) a Citinek vagy a Citi által kijelölt képviselőnek átadásra kerül (akár közvetlenül a Beszállító, akár a Letéti ügynök által a vonatkozó letéti megállapodás szerinti kötelezettségeinek teljesítése érdekében), akkor a Forráskódra és a Letétbe helyezett anyagokra a Beszállító és a Citi közötti vonatkozó megállapodás által meghatározott meglévő licenc érvényes, feltéve, hogy az egyes licencek feljogosítják a Citit a Forráskód és az egyéb Letétbe helyezett anyagok szükséges mértékű használatára és módosítására a következők érdekében: (i) a szoftvert és az egyéb Letétbe helyezett anyagokat a Citi rendszereivel integrálni, azok kompatibilitását biztosítani, (ii) a szoftver és az egyéb Letétbe helyezett anyagok Alkalmazandó jogszabályoknak, iparági szabványoknak és piaci gyakorlatnak való megfelelőségét biztosítani, (iii) lehetővé tenni, hogy a szoftver és az egyéb Letétbe helyezett anyagok naprakészek maradjanak a technológiai újítások fényében, és (iv) lehetővé tenni, hogy a szoftver és az egyéb Letétbe helyezett anyagok megfeleljenek a Citi és Leányvállalatainak üzleti céljainak a meglévő Licenc hatályán belül. A Szoftver bármely olyan verziójára, amely a Forráskód felhasználásával, a Citi által vagy nevében fejlesztett módosítást tartalmaz, a jelen Fejezet és az alapul szolgáló megállapodás összes rendelkezése alkalmazandó; mindazonáltal a módosítások tekintetében a Beszállító nem rendelkezik semmilyen joggal, tulajdonjoggal vagy érdekeltséggel, és a

módosításokhoz kapcsolódó összes szellemi tulajdonjog kizárólag a Citit illeti.

A Beszállító köteles a Szoftverben használt szoftvert biztosító harmadik felekkel együttműködve kereskedelmi tekintetben észszerű erőfeszítéseket tenni, hogy az ilyen harmadik féltől származó szoftverek forráskódját a Letétbe helyezett forráskódba foglalhassa. Ha a harmadik fél megtagadja a Beszállítónak e jog megadását, a Beszállító köteles kereskedelmi tekintetben észszerű erőfeszítéseket tenni, hogy az adott harmadik féltől származó szoftverlicenc-szerződés Megszűnési esemény esetén átruházható legyen a Citire.

Minden a Citinek a jelen Fejezet előírásainak megfelelően átadott Forráskódra az adott licencelt Szoftverre vagy a Hosztolt szolgáltatásra vonatkozó meglévő Licenc vonatkozik, *azzal a feltétellel*, hogy a Citi üzleti és működési követelményeivel összefüggésben jogosult felhasználni és módosítani a Forráskódot és a Szoftvert, hogy a Szoftver naprakész maradjon a technológiai újítások tükrében, és megfeleljen az Alkalmazandó jogszabályoknak. A Szoftver bármely olyan verziójára, amely a Forráskód felhasználásával, a Citi által vagy nevében fejlesztett módosítást tartalmaz, a vonatkozó megállapodás összes rendelkezése alkalmazandó; mindazonáltal a módosítások tekintetében a Beszállító nem rendelkezik semmilyen joggal, tulajdonjoggal vagy érdekeltséggel, és a módosításokhoz kapcsolódó összes Szellemi tulajdonjog kizárólag a Citit illeti.

15 GLOBÁLIS HÁTTÉR-ÁTVILÁGÍTÁSI SZABVÁNYOK

A jelen követelmények minden olyan külső beszállítóra vonatkoznak, amely szolgáltatásokat nyújt a Citi részére.

15.1 Áttekintés – Háttérellenőrzés

A háttérellenőrzést a vonatkozó helyi törvényeknek és szabályozásoknak megfelelően kell elvégezni. A jelen dokumentumban meghatározott valamennyi információt és önálló információszolgáltatást – az adott esetnek megfelelően – a Beszállító képviselőinek, munkavállalóinak és alvállalkozóinak kell rendelkezésre bocsátaniuk. Az információk meghamisítása vagy kihagyása, akár az önéletrajzon, akár az interjú alatt, a bejelentkezési űrlapon vagy a felvételi folyamat során, függetlenül attól, hogy azt mikor fedezik fel, a Citivel kapcsolatos megbízás megtagadását vagy megszüntetését eredményezheti, a helyi törvényeknek megfelelően. Ha bármely elvégzett átvilágítás kedvezőtlen eredménnyel zárul, függetlenül attól, hogy azt mikor fedezik fel, az szintén a Citivel kapcsolatos megbízás megtagadását vagy megszüntetését eredményezheti, a helyi törvényeknek megfelelően.

A háttérellenőrzés végrehajtásával kapcsolatos további információk az alábbi címen található:

https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

15.2 Alapvető információk begyűjtése, a személyazonosság ellenőrzése

Mielőtt bármely Beszállító munkatársa Citi-megbízásba kezdene, a Beszállító köteles feljegyezni az adott személy vezeték- és utónevét, postai címét és állandó lakcímét (ha

eltér), telefonszámát és e-mail-címét (ha van). A Beszállító Személyzetének a személyazonosságot igazoló dokumentumokat is be kell mutatniuk. Ez jelentheti nemzeti személyazonosító jel, kormány által kiállított fényképes személyazonosító okmány vagy útlevele adatainak és/vagy dokumentációjának megadását.

15.3 Szankciós szűrés

A Beszállító valamennyi, a Citi nevében munkát végző munkavállalóját, továbbá minden olyan Citi-beszállító legalább 25%-os tulajdonosát – beleértve az alvállalkozókat is –, függetlenül attól, hogy hozzáférnek-e a Citi adataihoz, rendszereihez, hálózataihoz és/vagy telephelyeihez, ellenőrizni kell az Amerikai Egyesült Államok Pénzügyminisztériuma Külföldi Eszközök Ellenőrzési Hivatala („OFAC”) által vezetett Különlegesen Kijelölt Állampolgárok és Tiltott Személyek („SDN”) listája, az Egyesült Államok által szankcionált régiók és joghatóságok listája, továbbá az Egyesült Államokon kívüli hatóságok által kibocsátott valamennyi vonatkozó szankciós lista – ideértve különösen az Európai Unió konszolidált pénzügyi szankciós listáját, az ENSZ Biztonsági Tanácsának konszolidált listáját, az Egyesült Királyság („UK”) szankciós listáját, valamint a helyi jogszabályok alapján alkalmazandó egyéb szankciós listákat („Egyesült Államokon kívüli szankciók”) – alapján.

Az OFAC-listák nyilvánosan elérhetők az alábbi weboldalon: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Bevándorlási jogszabályok betartása

A Beszállítónak igazolnia kell olyan eljárások működtetését és alkalmazását, melyekkel megerősíthető, hogy valamennyi munkavállaló jogosult munkavégzésének országában dolgozni. Ezen felül a Beszállító köteles a következőkre: (1) biztosítani kell, hogy valamennyi munkavállaló rendelkezzen a munkavégzéshez szükséges jogosultsággal, valamint (2) folyamatosan meg kell felelnie minden alkalmazandó jogszabálynak, rendeletnek és belső szabályzatnak, beleértve a munkavállalási jogosultságra és annak ellenőrzésére vonatkozó követelményeket is. A Beszállítónak továbbá igazolnia kell, hogy olyan eljárásokat működtet és tart fenn, amelyek biztosítják, hogy munkavállalói megfelelnek valamennyi alkalmazandó bevándorlási jogszabálynak és előírásnak, valamint rendelkeznek az általuk végzett feladatokhoz és tevékenységekhez szükséges megfelelő vízummal vagy tartózkodási jogállással.

15.5 Foglalkoztatási előzmények

A Beszállítók kötelesek igazolni személyzetük foglalkoztatási előzményeit hét (7) évre, illetve, ha a helyi szabályozás előírja, 10 évre visszamenőleg. Az egyének foglalkoztatási előzményeinek ellenőrzéséhez annak biztosítására van szükség, hogy a munkáltatók, beosztások, dátumok és feladatkörök pontosan lettek megadva. A Beszállító személyzetének ugyanakkor minden korábbi tanácsadóként vagy ideiglenes munkavállalóként, a Citinél vagy annak bármely elődállalatánál (beleértve, de nem kizárólagosan: Citibank, Citicorp, Travellers, Salomon Brothers és/vagy Smith Barney) való korábbi munkakapcsolatról (foglalkoztatás, megbízás, tanácsadás vagy ideiglenes munka) is be kell számolniuk.

15.6 Tanulmányi előzmények

A Beszállítók kötelesek bizonyítékot szolgáltatni a személyzetük által elért legmagasabb iskolai végzettségről. A validációnak ki kell terjednie az oktatás időpontjaira, az intézmény(ek) nevére és címére, és a megszerzett diplomára vagy diplomákra.

15.7 Bűnügyi háttér

Ha a jogszabályok megengedik, a Beszállító dolgozói és alvállalkozói kötelesek tájékoztatni a Citit, ha valamely bűncselekménnyel kapcsolatban letartóztatják, beperelik, beidézik, megvádolják vagy elítélik őket, beleértve a beismerő vallomást vagy „nolo contendere” nyilatkozattételt és a tárgyalás előtti diverziós vagy más hasonló programokat is. A bűnügyi háttér adminisztratív felülvizsgálatát és/vagy az ujjlenyomat-ellenőrzést a megbízás kezdete előtt el kell végezni, amennyiben ez jogilag megengedett és lehetséges. A lopással, csalással, tisztességtelen magatartással, bizalomsértéssel vagy más hasonló törvénysértéssel kapcsolatos bűncselekményekért kapott büntetőítéletek a Citivel kapcsolatos megbízás megtagadását és/vagy az arra való jogosultság elvesztését eredményezhetik (kivéve, ha ezt a jogszabályok tiltják). Az egyéb vonatkozású büntetőítéletek a vonatkozó helyi jogszabályok és előírások alapján a Citivel kapcsolatos megbízás megtagadását és/vagy az arra való jogosultság elvesztését eredményezhetik.

15.8 Ismételt átvilágítás

A Beszállító személyzetének azon tagjainál, akiknek a megbízása megszűnik, ismételten el kell végezni az átvilágítást, ha újra megbízzák őket a Citihez kapcsolódó feladatokkal. Az ismételt átvilágításra vonatkozó követelményekről itt található bővebb információ: https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Nemzetközi áthelyezések

Valamennyi átvilágítást a megbízás helye szerinti ország előírásaival összhangban kell elvégezni. Amennyiben a Beszállító bármely személyzeti tagját másik országba helyezik át, ismételten el kell végezni az adott személy átvilágítását az új ország követelményei szerint.

16 KÖLTSÉGEK

Beszállítók, akik szerződés alapján jogosultak visszatérítendő üzleti költségek igénylésére.

16.1 Áttekintés

A Citi csak azokat az észszerű üzleti jellegű költségeket téríti meg, melyeket előzetesen írásban jóváhagyott, és melyek a Beszállító részéről a Citinek nyújtott termékek és szolgáltatások kapcsán merültek fel, összhangban vannak a vonatkozó Szerződés vagy

a Citi Költségkezelési szabályzatának, valamint adott esetben a vonatkozó Szabványoknak és Eljárásoknak a feltételeivel, és melyeket a Citi által elfogadhatónak ítélt igazoló nyugták, számlák, útiterv vagy egyéb dokumentumok megfelelően alátámasztanak.

16.2 Visszatérítések

Ezeket a költségeket megfelelően dokumentálni, majd a Citinek a Citi számlázási követelményeinek megfelelően számlázni kell. A Citi alkalmazottai nem viselhetnek beszállítói költségeket egy Beszállító nevében. A Citihez benyújtott érvényes és jóváhagyott költségátalány vagy költségátalányok megtérítésére irányuló igénynek tartalmaznia kell (az összes egyéb számlázási követelményen túl) a következőket:

1. A költség üzleti célja;
2. A költség összege és leírása;
3. A költség helye és időpontja;
4. Azon projekt neve/leírása, melyhez a Beszállító szolgáltatásokat nyújt;
5. A Citi azon képviselőjének neve és Citivel való üzleti viszonya, aki a költségeket eredményező szolgáltatás(oka)t igényelte; valamint
6. A megrendelés száma, ha van.

A megtéríthető üzleti költségekkel kapcsolatos információkért kérjük, vegye fel a kapcsolatot elsődleges Citi üzleti kapcsolattartójával. A visszatérítési igényhez csatolni kell a Citi által elfogadhatónak ítélt igazoló nyugtákat, számlákat, útiterveket és egyéb dokumentációt. A visszatérítési igényléseknek meg kell felelniük a vonatkozó Szerződés rendelkezéseinek vagy, adott esetben, a Citi Költségkezelési szabályzatának és vonatkozó Szabványainak és Eljárásainak; az igényléseket jóvá kell hagynia a megfelelő üzleti támogatónak és/vagy az elsődleges Citi üzleti kapcsolattartónak, valamint egy olyan személynek, aki rendelkezik megfelelő felhatalmazással és az adott áru megvásárlásához elegendő kerettel. A nem megfelelő igénylések nem lesznek visszatérítve.

17 INFORMÁCIÓBIZTONSÁG (IS)

Azokra a Beszállítókra vonatkozik, beleértve az Alvállalkozókat is, akik eléri, feldolgozzák, tárolják vagy kezelik a Függelékben besorolt és meghatározott Citi-információkat; vagy Citi márkanevű internetes alkalmazásokért hosztként felelősek; vagy kapcsolódnak a Citi hálózati erőforrásaihoz; vagy kíséret nélküli hozzáférést igényelnek a Citi létesítményeihez.

17.1 Áttekintés

Jelen fejezet a Citi által elvárt információvédelmi minimumkövetelményeket ismerteti, melyek a Citi azon Beszállítóira vonatkoznak (beleértve a forgalmazó alfeldolgozókat és alvállalkozókat is), akik tárolják, feldolgozzák, kezelik a Citi-információkat vagy azokhoz hozzáférnek, akik Citi-alkalmazásokért hosztként felelősek, vagy a Citihez hálózati kapcsolattal rendelkeznek. Ezek a követelmények biztosítják az információk vonatkozó jogszabályok és szabályozási követelmények, valamint legmagasabb iparági normák (pl. ISO/IEC 27001/2) szerinti védelmét azokon a helyszíneken, ahol a Citi és annak Beszállítói üzletvitelt folytatnak. Ha a helyi jogszabályok, előírások vagy a releváns

iparági normák az itt foglaltaknál magasabb szintű elvárásokat támasztanak, akkor a Beszállítóknak ezeket a jogszabályokat, előírásokat vagy normákat kell követniük. Ezenkívül a Citi szabályzatainak és szerződéses feltételeinek való megfelelés részeként a Beszállítóknak esetlegesen további információbiztonsági gyakorlatokat és eljárásokat kell követniük. Ha a Beszállító úgy dönt, hogy további biztonsági gyakorlatokat vagy eljárásokat alkalmaz az információbiztonság érdekében, akkor a Beszállítónak gondoskodnia kell arról, hogy ezek a gyakorlatok és eljárások ne ütközzenek a jelen fejezetben meghatározott minimumkövetelményekkel.

17.2 Információbiztonsági politika és iránymutatás

A Beszállítóknak dokumentált információbiztonsági szabályzatokkal és szabványokkal kell rendelkezniük. A szabályzati iránymutatásnak tartalmaznia kell a szerep- és felelősségi körök egyértelmű meghatározását, valamint a szabályzatok és normák éves felülvizsgálatát és frissítését a technológia aktuális állásával, az iparági szabványokkal, valamint a jogi és szabályozási követelményekkel való összhang érdekében.

17.3 Feladatok szétválasztása

A Beszállítónak olyan folyamatokkal kell rendelkeznie, amelyek biztosítják, hogy megfelelő felhatalmazás vagy azonosítás hiányában egyetlen személy se tölthessen be ugyanazon tevékenységhez, változtatáshoz, információs rendszerhez vagy tranzakcióhoz kapcsolódóan egyszerre két üzleti funkciót, két informatikai funkciót vagy két, az Ellenőrzött Információs Rendszerhez tartozó funkciót tartós hozzáféréssel, kivéve, ha megfelelő kompenzációs kontrollok állnak rendelkezésre a kockázat mérséklésére.

A. táblázat

Funkciók	Funkcióleírás
Fejlesztői / Mérnöki munka	Szoftverek, hardverek és konfigurációk tervezése, létrehozása vagy módosítása; például: - Új alkalmazáskód és a hozzá kapcsolódó adatbázissémák megtervezése és létrehozása - Infrastruktúra-termékek és alkalmazáskomponensek fejlesztése - Technológiai termékek testreszabása a szoftverekkel és szolgáltatásokkal történő integráció érdekében
Jóváhagyás	A bevezetésre kerülő programkód-módosítások jóváhagyása
Rendszerek bevezetése / adminisztrációja	Szoftverek, hardverek és konfigurációs módosítások telepítése, bevezetése vagy adminisztrációja. Például: - Programkód éles környezetbe történő automatikus vagy manuális telepítése

	- Technológiai termék vagy berendezés telepítése - Szolgáltatások indítása vagy leállítása az éles környezetben működő rendszerek hibakeresésének és helyreállításának támogatása érdekében
Kiemelt jogosultságú azonosítókhoz fűződő tevékenységek felülvizsgálata	A változáskezelési tevékenységek vagy a biztonsági események (például auditnaplók) ellenőrzése
Azonosítók kezelése	Felhasználói azonosítók (felhasználók, FID-ek és botok), jogosultságok vagy jelszavak létrehozása, módosítása és törlése
Üzleti funkció	Funkcióleírás
Üzleti tranzakció kezdeményezése	Üzleti tranzakciók kezdeményezése (más néven rögzítése, létrehozása vagy bevitele), valamint ügyfeladatok módosítása
Üzleti tranzakció jóváhagyása	Üzleti tranzakciók jóváhagyása (más néven engedélyezése, ellenőrzése vagy véglegesítése)
Informatikai funkció	Funkcióleírás
Hálózatüzemeltetés	A hálózati infrastruktúra-szolgáltatásokat nyújtó eszközök üzemeltetése kezelése és működésük támogatása. Ilyen eszközök például a hálózati útválasztók, kapcsolók, tűzfalak és a tartománynév-szolgáltatások (DNS)
Nem hálózati üzemeltetés	Az olyan eszközök üzemeltetése, kezelése és működésük támogatása, amelyek nem nyújtanak hálózati infrastruktúra-szolgáltatásokat. Ilyen eszközök például a szerverek, telefonok és számítógépek

17.4 Vezetőségi információbiztonsági kötelezettség

Azokra a Beszállítókra nézve, akik Citi márkanévű internetes alkalmazásokért hosztként felelősek, és/vagy akik hozzáféréssel rendelkeznek bizalmas vagy magasabb besorolású Citi-információkhoz, kötelező érvényű a Citi Harmadik felekre vonatkozó információbiztonság-kiértékelési folyamata (TPISA); e folyamat keretében megállapításra kerül, hogy a Beszállító szabályzatai, eljárásai és ellenőrzésre szolgáló eszközei mennyire felelnek meg a Citi követelményeinek, valamint az információbiztonságra vonatkozó (a Citivel vagy a Beszállítóval szembeni) jogi és/vagy szabályozási követelményeknek.

Az értékelés a Beszállító által kitöltendő, alátámasztó bizonyítékkal kiegészített biztonsági kérdőívekből, valamint esetlegesen a Beszállító azon helyszíneinek meglátogatásából áll, ahol a Citi bizalmas vagy magasabb besorolású információit tárolja, feldolgozza, kezeli vagy eléri a harmadik fél. Ezenkívül a TPISA Harmadik Felekért Felelős Folyamatos Megfigyelő Csoportja kiberbiztonsági megfigyelőeszközökkel figyelheti meg a Beszállítót, nyilvánosan elérhető információkat használva a sebezhető, internetre irányuló rendszerek, hosztok, alkalmazások és szerverek azonosítására, mindezt olyan dolgok tekintetében, mint az élettartamuk végét elérő szoftverek, kihasznált nyitott portok, sebezhetőségek és egyéb veszélyforrások. Ha a TPISA biztonsági hiányosságokat fed fel vagy jelez, akkor a Citi egy, a Beszállítónak küldött értesítésben dokumentálja az eredményeket, és a Beszállítóval együttműködve megpróbálja megállapítani, hogyan lehet orvosolni az adott hiányosságokat. A Beszállítók kötelesek haladéktalanul elvégezni a szükséges korrekciókat és/vagy bevezetni a szükséges kompenzáló ellenőrzéseket a Citi aggályainak a Citi saját kizárólagos belátása szerint elfogadható mértékű kezelésére, és betartani az előírt határidőt, amely Magas kockázatú problémák esetén 180, Közepes kockázatú problémák esetén 240 naptári nap, Alacsony kockázatú problémák esetén pedig a következő kiértékelés dátuma. A kockázatok besorolását a Citi állapítja meg.

1. A Beszállító köteles rendszeresen kiértékelni üzleti műveleteit és a kapcsolódó ellenőrzéseket saját információbiztonsági szabványai, szabályzatai és eljárásai alapján. Az időszakos kiértékeléseknek legalább az alábbiakra ki kell terjedniük:
 - a) Azoknak a folyamatoknak a kiértékelése, amelyeket a Beszállító a saját információbiztonsági szabályzatának és szabványainak való megfelelés biztosítására alkalmaz;
 - b) Azoknak a támogató erőforrásoknak, például a Beszállító által használt alkalmazásoknak és infrastruktúrának, valamint a Beszállító alvállalkozói által használt információbiztonsági folyamatoknak (ha vannak) az értékelése, melyek támogatják üzleti tevékenységüket, vagy lehetővé teszik a Citi számára az ilyen értékelések elvégzését. Megfelelés szükséges abban az esetben, ha egy harmadik fél olyan alvállalkozóval ír alá új szerződést vagy újít meg meglévő szerződést, aki hozzáféréssel rendelkezik a Citi besorolása szerint Bizalmas vagy magasabb szintű Citi-információkhoz, azokat feldolgozza, kezeli vagy megsemmisíti.
2. A valamely információbiztonsági kockázatelemzés (pl. TPISA) által felderített problémákat dokumentálni kell, illetve lezárásig nyomon kell követni, a helyreállítás bizonyítékát pedig a Citi rendelkezésére kell bocsátani.
3. Ha a Beszállító az információbiztonság kezeléséért felelős funkciót egy másik országba helyezi át, akkor a Citi dokumentált jóváhagyására van szükség az áthelyezést megelőzően.
4. Ha a Beszállító új vállalatot vásárol fel, akkor a Beszállítónak el kell végeznie az új vállalat kiértékelését annak ellenőrzésére, hogy az megfelel-e a jelen Szabványoknak.
5. A Citi előzetes írásbeli hozzájárulása nélkül a Beszállítónak tilos kiszervezni a Citi-információk tárolásához, feldolgozásához és/vagy továbbításához használt rendszerek biztonságáért, többek között, de nem kizárólagosan a tűzfalak, a

rendszerbeállítások és a javítócsomagok kezeléséért vagy az információbiztonság adminisztrálásáért (ISA) felelős funkciókat.

6. Ha a Beszállító Citi-információkat tartalmazó vagy a Citi védjegye alá tartozó szoftvert vagy webhelyet üzemeltet, akkor rendszeres kiértékeléseket kell végeznie azok sebezhetőségéről a Citi Rendszerbiztonság-tesztelés (SSTS) normájának megfelelően, és a kiértékelés során talált lényeges hibákat orvosolnia kell a normában meghatározott határidőkön belül. Mivel az SSTS-t nem hagyták jóvá külső terjesztésre, a Beszállítóknak a hozzájuk tartozó Citi ügyfélkapcsolati felelőssel kell együttműködniük a referenciadokumentumoknak való megfelelés biztosítása érdekében. Ezen túlmenően a Beszállítónak meg kell felelnie a vonatkozó ISO/IEC 27001 Információbiztonsági irányítási szabványoknak (vagy az azok helyébe lépő, magasabb követelményeket és protokollokat megállapító információbiztonsági irányítási szabványoknak), és be kell tartania a jelen (17.) fejezetben foglalt információbiztonsági rendelkezéseket.
7. Ha a Citi belső hálózatán kiszolgálókhöz és/vagy információs rendszerekhez való csatlakozásra van szükség, akkor a Beszállító erről köteles értesíteni az elsődleges Citi üzleti kapcsolattartóját az aktuális csatlakozási folyamat követése érdekében.
8. A Beszállító köteles haladéktalanul értesíteni a Citi megfelelő kapcsolattartóját (az üzleti tevékenységért felelős személyt (BAO)) a Citi-információkhoz való jogosulatlan hozzáférésről, azok jogosulatlan megszerzéséről, elvesztéséről, sérüléséről vagy törléséről, illetve a Citi-információk tárolására, feldolgozására vagy továbbítására használt információs rendszerekkel kapcsolatos bármely más jellegű sérülésről.
9. A Beszállító köteles gondoskodni arról, hogy minden magas kockázatú tevékenység és az érzékeny adatok valamennyi módosítása rendelkezzen ellenőrzési nyomvonallal, mely lehetővé teszi azok végrehajtó személyhez való hozzákapcsolását.
10. A Beszállítónak biztosítania kell az összes bizalmas vagy magasabb besorolású adat elfedését képernyőkön és papíron egyaránt (többek között például az ellenőrzési, a kivételes, a törvényi és az egyéb jelentéseken).
11. A Beszállító köteles korlátozni az érzékeny adatok nyomtatását, rögzítését és másolását, ideértve a saját eszközökkel végzett műveleteket is. A Beszállító köteles a megállapodás alatt előre egyeztetett időpontban vagy annak végén az összes Citi-információt visszaszolgáltatni vagy megsemmisíteni, kivéve, ha ezt törvény vagy szabályozás tiltja.
12. A Beszállító köteles biztosítani, hogy a Citi-információkhoz hozzáféréssel rendelkező személyzeti tagjai (alkalmazottak, vállalkozók, ideiglenes alkalmazottak, alvállalkozók) titoktartási megállapodást írjanak alá.
13. A Beszállító alkalmazottainak biztosítani kell alkalmazotti kézikönyvet vagy hasonló dokumentumot, mely leírja a Beszállító a betanulási folyamat során elfogadott magatartási kódexének és humánerőforrás-politikájának megsértése esetén követendő fegyelmi eljárást.
14. A Beszállítónak eljárással kell rendelkeznie arra, hogy egy alkalmazott vagy nem alkalmazott felmondása vagy elbocsátása esetén minden eszközt visszaszerezzen.
15. Amennyiben Bizalmas információ webhelyen vagy weben hozzáférhető rendszeren van fenntartva vagy bármilyen módon tárolva, úgy ezt a Beszállítónak közölnie kell a Cítivel. Ez a közlés szerepelhet a Szolgáltatások leírásában is. Ha

a Beszállító Bizalmas Citi-információkat tart fenn vagy tárol, akkor a jelen Megállapodás időtartama alatt a Beszállító évente egyszer köteles SSAE 18 auditot (vagy bármely annak helyébe lépő, a Citi által jóváhagyott irányadó kiértékelést) végezni, valamint legalább évente egyszer átadni a Citinek az ilyen SSAE 18 audit vagy bármely annak helyébe lépő, a Citi által jóváhagyott irányadó kiértékelés eredményeit dokumentáló jelentések egy példányát.

16. Ha a Beszállítót egy összeolvadás, felvásárlás vagy hasonló ügylet keretében felvásárolják vagy a Beszállító felvásárol egy másik jogi személyt, és az ilyen tranzakció hatással lehet a Szolgáltatásokra, akkor a Beszállító köteles haladéktalanul írásban értesíteni a Citit, továbbá a Beszállítónak el kell végeznie a létrejövő szervezet kapcsán egy jelen Követelményeknek megfelelő információbiztonsági értékelést, annak biztosítása érdekében, hogy az összeolvadás vagy felvásárlás ne legyen hatással az ezeknek való megfelelésre.

17.5 Alvállalkozói információbiztonsági kockázat

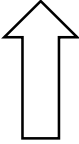
A Beszállítónak elő kell írnia az ügyfeladatokhoz hozzáférő alvállalkozóknak a szerződéskötés előtt, illetve szerződéskötés után rendszeresen, szakképzett Információbiztonsági (IS) személyzettel elvégzett Információbiztonsági felméréseket. Ezeket a felméréseket a vezetőség által jóváhagyott folyamatnak megfelelően kell elvégezni, mely az értékelési eljárás minden szakaszára kiterjed, a kezdeményezéstől a problémakezelésig. Az alvállalkozói információbiztonsági értékelésnek tartalmaznia kell a Citi Harmadik felekre vonatkozó információbiztonsági felmérési kérdőívének (TPAQ) megfelelő és az alvállalkozó információbiztonsági teljesítményét felmérő kérdőívet vagy azzal egyenértékű eszközt, és egy logikai módszert az alvállalkozó bevonásával kapcsolatos információbiztonsági kockázat kiszámítására. A Beszállító köteles a lezárásig nyomon követni az értékelés teljesítését, és kezelni a megállapított problémákat és a korrekciós intézkedési terveket.

17.6 Felelősség az eszközökért

1. A Beszállítónak gondoskodnia kell egy, az összes olyan alkalmazást és hardvert magában foglaló nyilvántartás vezetéséről, amelyet Citi-információk tárolására, feldolgozására és/vagy továbbítására használnak.
2. A Beszállítónak gondoskodnia kell arról, hogy a Citi információs eszközeinek nyilvántartását az irányítása alatt tartsa, a nyilvántartás pontosságának és teljességének megfelelő fenntartását szolgáló eljárással összhangban.
3. A Beszállítónak kell felelősnek lennie az ellenőrzése alatt álló összes Citi-információ védelméért.
4. A Beszállítónak biztosítania kell a felhasználók tevékenységének elszámoltathatóságát az iparági gyakorlatnak megfelelő módon.
5. A személyes külső internetes e-mailes és felhőalapú tárolási fiókokhoz való felhasználói hozzáférést korlátozni kell a Beszállító azon globális hálózataról, ahol a Citi-információ található.

17.7 Információ besorolása és kezelése.

A Citi az alábbi információbesorolási táblázat szerint sorolja be az információkat. Az alább felsorolt információbesorolások definíciója és példái a Függelékben találhatók.

KORLÁTOZOTT HOZZÁFÉRÉSŰ	Legérzékenyebb
ÉRZÉKENY PII	
BIZALMAS PII	
BIZALMAS	
BELSŐ PII	
BELSŐ	
NYILVÁNOS	Legkevésbé érzékeny

1. A Citi-információk besorolása alapján a Citinek együtt kell működnie a Beszállítóval az ilyen információk védelméhez szükséges biztonsági szint megállapításában; a Beszállító köteles gondoskodni a megfelelő ellenőrzések meglétéről, valamint a Citi által előírt esetleges megemelt vagy módosított besorolások követelményeiről.
2. A belső vagy magasabb besorolású Citi-információkat olyan harmadik felek által kezelt eszközökön kell tárolni, melyeket a Harmadik fél és a Citi közti, a Citi irányelveinek és normáinak megfelelő titoktartási rendelkezéseket tartalmazó szerződés szabályoz.
3. Ha a Beszállító lehetővé teszi a Citi-adatok tárolását nem a vállalat tulajdonában lévő eszközökön (vagyis 4. fél által kezelt eszközökön), akkor a Beszállítónak rendelkeznie kell konkrét vezetői jóváhagyást megkövetelő irányelvvel, valamint kidolgozott iránymutatással és ellenőrző eljárásokkal a Citi-információk használatára és megsemmisítésére vonatkozóan.
4. A Beszállító köteles minden esetben biztosítani a Citi-információk jogosulatlan hozzáféréssel, módosítással és törléssel szembeni védelmét.
5. Az elektronikus adathordozón továbbított bizalmas vagy magasabb besorolású Citi-információkat jóváhagyott kriptográfiai algoritmussal kell titkosítani, és az átvételt vissza kell igazolni. A Beszállítónak meg kell győződnie arról, hogy a címzett megkapta az elektronikus adathordozót. Ha a kézbesítés várható időpontjáig nem érkezik meg az átvételről szóló visszaigazolás, akkor a Beszállító köteles értesíteni a Citit.

17.8 Biztonságos konfiguráció.

1. A Beszállító köteles dokumentált, biztonságos konfigurációs szabványt fenntartani minden olyan eszközt illetően, melynek segítségével lehetséges a Citi-információk tárolása, feldolgozása, az azokhoz való hozzáférés, illetve azok továbbítása.
2. A Beszállítónak információbiztonsági ellenőrzésekkel kell kiegészítenie saját eljárásait és folyamatait az alkalmazások, termékek és szolgáltatások kiválasztására, fejlesztésére és bevezetésére vonatkozóan.
3. A Beszállítónak biztonságos kidolgozási eljárással kell rendelkeznie a Citi-információk tárolására, feldolgozására és/vagy továbbítására használt valamennyi rendszer esetén.
4. A Beszállító köteles minden rendszerhez biztonságos képet vagy sablont fenntartani.

5. A forgalmazó által támogatott rendszereken, hálózati eszközökön és alkalmazásokban minden alapértelmezett felhasználói fiókot és jelszót el kell távolítani és/vagy módosítani kell.
6. Minden feltört rendszert vagy szolgáltatást egy olyan kép vagy sablon használatával kell újraépíteni és konfigurálni, amely bizonyítottan integritással rendelkezik.
7. A biztonságos konfigurációkon végrehajtandó összes változtatást jóvá kell hagyatni a vezetőséggel a Beszállító változáskezelési folyamatán keresztül.
8. A Beszállító a biztonságos konfiguráción végrehajtott minden változásáról köteles értesíteni a Citi-t.
9. A biztonságos kidolgozási eljárásnak magában kell foglalnia a biztonsági/standard kidolgozási beállítások termelésbe történő bevezetésekor végrehajtandó automatizált konfiguráció-ellenőrzést támogató eszközöket, valamint az alapkonfigurációnak való megfelelés és az attól való eltérések folyamatos felügyeletét.

17.9 Titkosítási követelmények

A Beszállító Bizalmas vagy annál magasabb minősítésű információt nem továbbíthat titkosítás nélkül. A Bizalmas vagy annál magasabb minősítésű információkat a Citi által jóváhagyott eszközökkel vagy megoldásokkal, **végpontok közötti** (end-to-end) titkosítással kell védeni. A titkosított adattovábbításhoz jóváhagyott protokollok és azok elfogadott verziói a következők:

1. Hitelesítési és hitelesítési adatok cseréjekor: SAML v2.0, OAuth v2.0 (csak hitelesítés),
2. A kommunikációs csatornák és a kapcsolódó kulcscsere védelme érdekében kizárólag az alábbi hálózatbiztonsági protokollok alkalmazhatók:
 - a) A TLS 1.3 használata az elsődlegesen ajánlott, és a TLS 1.3 valamennyi titkosítási csomagja engedélyezett. Ha kizárólag a TLS 1.3 protokoll engedélyezett, további felülvizsgálatra nincs szükség.
 - b) Ha a TLS 1.3 alkalmazása műszaki okokból nem megvalósítható, és TLS 1.2 használata történik, akkor az SSL Labs által adott B vagy annál jobb minősítés elfogadható, és ebben az esetben sincs szükség további felülvizsgálatra.

A Citi harmadik felek környezetében tartósan tárolt adatokat, illetve azok cseréjét teljes mértékben titkosítani kell Citi által jóváhagyott eszközökkel vagy megoldásokkal. Az adatok titkosítására jóváhagyott algoritmusok és kulcshosszok a következők:

1. **Speciális titkosítási szabvány (AES):** Jóváhagyott kulcshosszok: 256 vagy több bit. Korlátozott módok: Az Elektronikus kódkönyv (ECB) üzemmód tiltott, kivéve, ha a sima szöveg mennyisége kisebb vagy egyenlő a blokkhosszal. Lemez meghajtó titkosítása: 256 bites kulccsal rendelkező AES-re van szükség. A 128-bites kulcshosszúságú AES algoritmus TLS titkosítási algoritmusként jelenleg még alkalmazható, azonban 2028. december 31-től nem lesz elfogadható, helyette kizárólag 256-bites vagy annál nagyobb kulcserősségű titkosítás alkalmazható, hogy a Citi összhangba kerüljön a nemzetközi átállási ütemtervekkel (hiv.: NIST IR 8547 IPD).

2. **ChaCha20 (folyamkódolás kapcsolódó használati esetekhez):**
Jóváhagyott kulcshosszok: 128 vagy 256 bit, 96 bites egyszer használatos kulccsal és 32 bites blokkszámmal, vagy 64 bites egyszer használatos kulccsal és 64 bites blokkszámmal. Maximális adatméret: 16 petabájt.

A jóváhagyott nyilvános kulcson alapuló titkosítási rendszerek, a kulcscsere, a megállapodási mechanizmusok, az üzenetkivonati és kulcsszármaztató funkciók a következők:

A Beszállító kvantumfelkészültségével kapcsolatos közlemény: A Beszállítóknak be kell mutatniuk a NIST IR 8547 (ipd) 2. és 4. táblázatának tartalmára vonatkozó tervüket a Citi Kvantumfelkészültségi Program csapatának a következő címen keresztül: ([felmérés linkje](#)).

1. **Nyilvános kulcsú kriptorendszerek és minimális kulcshosszok:**
 - a) Rivest–Shamir–Adleman (RSA): 2048 bit.
 - b) Digitális aláírási algoritmus (DSA): 2048 bit. A DSA-t tilos a Citin kívül feldolgozott vagy tárolt Citi-adatok védelmére használni.
 - c) Elliptikus görbéken alapuló digitális aláírási algoritmus (ECDSA): 256 bites, valamint az ANSI X9.62 szabványban meghatározottak szerint a NIST által ajánlott görbékkel.
2. **Kulcscsere- és megállapodási mechanizmusok és minimális kulcshosszok:**
 - a) Diffie-Hellman (DH) / Ideiglenes Diffie-Hellman (DHE): 2048 bit.
 - b) Diffie-Hellman elliptikus görbe (ECDH) / Diffie-Hellman ideiglenes elliptikus görbe (ECDHE): 256 bites, valamint az ANSI X9.63 szabványban meghatározottak szerint a NIST által ajánlott görbékkel¹.
3. **Üzenetkivonati függvények:** Tilos olyan titkosítási kulcsot létrehozni, amelynek hosszúsága meghaladja a hash generálásához használt anyagban található véletlenszerű bitek számát.
 - a) SHA-1 Kizárólag nem digitális aláírásos alkalmazásokhoz elfogadható. SHA-2-család, SHA-3-család és POLY-1305: Minden hash-függvényes kriptográfiai alkalmazáshoz elfogadható.
4. **Jelszó alapú kulcsszármaztató függvények és minimális követelmények:**
 - a) PBKDF2: Minimum 10000 iteráció, legalább 16 bájtos salt értékkel.
 - b) HKDF: Salt értékkel kell ellátni, és tartalmaznia kell az információ inputértéket.
 - c) SCRYPT: Minimum körök száma/költségtényező: 10.
 - d) Adatfolyam-titkosításhoz tilos a NIST SP800-108 KDF használata. A NIST SP 800-108 KDF módok, nevezetesen a Számláló, a Visszacsatolás és a Dupla Pipeline Iterációs módok elfogadhatók.
 - e) Az Argon2 javasolt.
5. **Jelszókivonat-funkciók és minimumkövetelmények:**
 - a) Bcrypt (a hitelesítési anyagok helyi tárolására): Minimum körök száma/költségtényező: legalább 10.

¹ Az ECDHE a preferált.

- b) Az Argon2 vagy a PBKDF2 használata ajánlott jelszókivonatoláshoz, ha a jelszavakat helyben tárolják a Beszállító valamely termékének részeként telepített környezetben vagy rendszeren.

17.10 Külső e-mail

Az olyan Bizalmas vagy magasabb besorolású Citi-információkat tartalmazó egyéni e-mailek esetén, amelyek vonatkozásában – az előírások és/vagy a Beszállító irányelve értelmében – nem megengedett Citi által jóváhagyott végpontok közötti titkosítási szoftver vagy eszköz használata, a titkosítási követelmények teljes körű teljesítéséhez átvitel-titkosítás (pl. Transport Layer Security (TLS) protokoll révén elvégzett gatewayek, azaz átjárók közötti titkosítás) alkalmazható. A jóváhagyott biztonságos e-mail-protokollok a következők:

1. **Azonosításon alapuló titkosítás (IBE):** biztonságos e-mail-funkcióval rendelkezik és alkalmazható a Citi ügyfélszolgálati megoldásaiban, valamint a biztonságos e-mailes és eDelivery rendszerekben.
2. **Kötelező TLS (MTLS):** munkamenet-titkosítás funkcióval rendelkezik (nem titkosítja az e-mail adattartalmát) és olyan forgalmazók, partnerek és ügyfelek esetében lehet alkalmazni, akik megállapodás keretében előre letárgyalták ennek használatát.
3. **Domain-kulcsokkal azonosított levél (DKIM):** hitelesítési és kulcskezelési funkcióval rendelkezik, és forgalmazók, partnerek és ügyfelek esetében lehet alkalmazni.

17.11 Privát hálózatok

Az elismert hatóság által függetlenül szabályozott és a pénzügyi szolgáltatási ágazat szabványainak megfelelő privát hálózatok mentesülhetnek a bizalmas, személyazonosításra alkalmas adatok átvitel közbeni titkosítására vonatkozó követelmény alól, amíg ezek a hálózatok nem rendelkeznek a titkosított adatátvitel teljes körű támogatásához szükséges infrastruktúrával.

17.12 Hangátvitel és fax

A Bizalmas vagy magasabb besorolású Citi-információk faxon történő küldése vagy hanghívások révén történő megvitatása (beleértve az IP-alapú hanghívást [VOIP] is) titkosítás nélkül is megengedett. Szükség esetén a Beszállítónak speciális eljárásokat és útmutatásokat kell kidolgoznia az ezeken a csatornákon keresztül továbbított Bizalmas vagy magasabb besorolású információk védelmére.

17.13 Kriptográfiai kulcs- és tanúsítványkezelés

A jelen fejezet használatában a biztonságos határ kifejezés egy kriptográfiai modul-érvényesítési program (CMVP), például a szövetségi információvédelmi szabvány (FIPS) által hitelesített határt jelent (a FIPS 140-2/3 által előírt 2. szint a minimálisan elfogadható biztonsági szint). (A bizalmas számítástechnikai enklávék, például az AWS Nitro enklávék elfogadhatók. Más különleges biztonsági esetekben jóváhagyást kell kérni a Cititől).

1. A Beszállítónak a titkosításra és az aláírásra az aktuális iparági szabványoknak megfelelő kriptográfiai algoritmusokat és minimális

kulcshosszokat kell alkalmaznia (beleértve az SSH-kulcsokat is). A Beszállítónak a változáskezelési folyamatán keresztül garanciát kell vállalnia arra, hogy az ilyen algoritmusok és kulcshosszak az egyes frissítések után is megfelelnek az iparági szabványoknak.

2. A Beszállítónak hivatalosan dokumentált kulcs-, titok- és tanúsítványkezelési életciklusra vonatkozó folyamattal kell rendelkeznie, olyan ellenőrzési eszközökkel, amelyek megvédik az érzékeny anyagot a jogosulatlan felhasználástól és a kitettségtől. Valamennyi kriptográfiai titok és a kulcsok életciklusával kapcsolatos művelet kizárólag biztonságos védelmi határon belül történhet. Az emelt szintű és biztonságos határokhoz való minden hozzáférést dokumentálni kell. A Beszállító köteles szekvenciadiagramot biztosítani a kulcs összes életciklus-eseményéről, kiemelve az érintett szereplőket, entitásokat és határokat.
3. A kriptográfiai kulcsoknak egyedi céllal kell rendelkezniük, és tilos felhasználni őket bármilyen egyéb célra, például ugyanazt a titkosítási kulcsot lemeztitkosításhoz és adattitkosításhoz, vagy ugyanazt a titkosítási kulcsot a hasznos adatok titkosításához és az adatbázisok titkosításához. SaaS-szolgáltató által ugyanazon kriptográfiai kulcs több ügyfél közötti újrafelhasználása alapértelmezés szerint tilos. Ez kizárólag olyan nem kritikus, alacsony kockázatú felhasználási esetekben engedélyezhető, amelyek a Bizalmas PII, Érzékeny PII és Korlátozott minősítési szint alatti Citi-információkat érintenek, és kizárólag a Biztonsági Architektúra Tanács kifejezett jóváhagyásával.
4. A (szimmetrikus vagy aszimmetrikus) kriptográfiai kulcsoknál a titkos kulcsot vagy a titkos kulcsanyagot (például a magokat vagy a titkos kulcs egy részét) minden esetben tilos nem titkosított szöveg formájában megjeleníteni. A titkos kulcs vagy a titkos kulcsanyag (például a kulcsmagok vagy a titkos kulcs egy része) soha nem hagyhatja el a biztonságos határt, kivéve az átmeneti kulcsokat, például a dinamikus munkamenetkulcsokat. Ha a kialakítás megköveteli egy szimmetrikus vagy titkos kulcs használatát, vagy egy titkos kulcs anyag biztonsági enklávék/privilegizált hozzáférést igénylő határok közötti továbbítását, akkor azt kizárólag szimmetrikus kulcs-rejtjelező kulcs vagy nyilvános kulcsú szállítókulcs használatával titkosított formában, kölcsönös TLS-titkosított alagutakon keresztül lehet továbbítani, és a továbbítást írásban jóvá kell hagyatni a Cíttel. Ezekben az esetekben a privát kulcsú Szállítókulcs soha nem hagyhatja el azt a privilegizált hozzáférést igénylő biztonságos határt, ahol generálták.
5. A szimmetrikus kulcs-rejtjelező kulcsot két vagy több kulcskomponensre kell felosztani, és XOR műveletet kell végrehajtani rajtuk a kibocsátás előtt, illetve kézi kulcsbevitelhez/betöltéshez. A szimmetrikus kulcs-rejtjelező kulcsnak megfelelő hozzáférés-vezérlési listákkal (ACL-ekkel) kell rendelkeznie a biztonságos határon belül, mint amilyenek a CMVP programmal ellenőrzött modulok; a szimmetrikus kulcs-rejtjelező kulcs soha nem tárolható a biztonságos határon kívül.
6. Az emberek, szolgáltatások és automatizált ügynökök hozzáférését a kulcstárakhoz, illetve a titkos kulcsokat, titkokat és titkos kulcsanyagot (például kulcsmagot vagy titkos kulcs egy részét) tartalmazó titkos határokhöz megfelelően el kell különíteni olyan vezérlőkkel, amelyek kizárólag az arra jogosult személyekre vagy rendszerekre korlátozzák a hozzáférést.

7. Minden kérést a titkos vagy szimmetrikus kulcsokat tartalmazó kulcstárakhoz való hozzáféréshez naplózni és dokumentálni kell ellenőrzési célokból, például olyan részletekkel, hogy ki, mikor és miért kérte a hozzáférést.
8. A Beszállító nem használhat saját maga által aláírt tanúsítványokat, univerzális tanúsítványokat vagy alapértelmezett SSL-tanúsítványokat.
9. Valamennyi kriptográfiai kulcs esetében meg kell határozni a kulcs érvényességi időtartamát a NIST SP800-57 Part 1, Revision 6 ajánlásának megfelelően. A kulcsokat a lejárat előtt frissíteni vagy váltani kell, hogy alkalmazkodjanak a változásokhoz, egyeztetési problémákhoz és a rendszer fagyásához szükséges időhöz.
 - a) Lejárt tanúsítvány cseréjekor tilos a régi aszimmetrikus kulcspárok újrafelhasználása.
10. A kriptográfiai kulcsokat kompromittálódottnak kell tekinteni, amint felmerül a gyanú, hogy a kulcs integritása, a kulcs tárolására vagy megosztására szolgáló közeg, illetve a szimmetrikus vagy privát kulcs bizalmassága veszélybe került. Minden veszélyeztetett kulcs üzemi használatát meg kell szüntetni, és az összes kapcsolódó tanúsítványt vissza kell vonni.
11. A vezetékek nélküli hálózatokat az iparági szabványoknak megfelelő titkosítási algoritmusokkal kell titkosítani.
12. A kriptográfiai mechanizmusok bármilyen formáját alkalmazó Beszállítóknak az iparági szabványoknak megfelelő kulcskezelési eszközöket és technikákat kell alkalmazniuk. A kulcskezelési szerepkört el kell különíteni a műveletek kezelésétől.
13. A Beszállítók kizárólag akkor alkalmazhatnak felhőnatív KMS- és PKI-szolgáltatásokat, ha biztosított azok együttműködése a Citi Data Security Services által biztosított PKI- és KMS-szolgáltatásokkal, és a kriptográfiai felügyelet nem kerül a Citi kriptográfiai irányítási keretrendszerén kívülre.

17.14 Hozzáférés-vezérlési felelősség

A Citi Bizalmas vagy magasabb besorolású információinak tárolására, elérésére, kezelésére, feldolgozására vagy továbbítására használt összes Ellenőrzött információs rendszer védelme érdekében a Beszállító köteles érvényesíteni a legkisebb jogosultság elvét azáltal, hogy minden egyes beosztás tekintetében a minimális hozzáférési szintre korlátozza a felhasználói jogosultságokat, valamint az összes rendszerhez és alkalmazáshoz való logikai hozzáférés biztosításának irányításával. Az ellenőrzéseknek teljes mértékben dokumentálnak és auditálhatónak kell lenniük. A hozzáférések biztosítását és megszüntetését – beleértve a jelszó-visszaállítást és a felhasználói fiókok engedélyezését is – lehetőség szerint automatizált folyamatok útján kell végrehajtani annak érdekében, hogy csökkenjen a túlzott jogosultságokból és az emberi hibákból eredő kockázat, valamint biztosított legyen az iparági szabványoknak való megfelelés.

1. A Beszállító felelős a szervezetén belüli összes felhasználó hozzáférési jogaiért.
2. A Beszállítónak olyan hozzáférés-vezérlő eszközöket kell alkalmaznia, amelyek biztosítják, hogy a felhasználók kizárólag a feladataik elvégzéséhez feltétlenül szükséges kiváltságokat és jogosultságokat kapják meg.

3. A Beszállító köteles bevezetni egy olyan eljárást, amely révén biztosítható, hogy az illetéktelen használat megelőzése érdekében minden alapértelmezett hozzáférési lehetőség eltávolításra, letiltásra vagy védelmezésre kerüljön.

17.15 Felhasználói hozzáférés kezelése

A Bizalmas vagy magasabb besorolású Citi-információkat feldolgozó, tároló és/vagy továbbító rendszerekhez és alkalmazásokhoz tartozó logikai hozzáférések kiosztását a Beszállítónak kell kezelnie. Ezek közé tartoznak a következők:

1. Jóváhagyott hitelesítési rendszerek azonosítása és nyilvántartása.
2. Annak megkövetelése, hogy a Citi-adatokhoz való hozzáféréshez minden esetben szükség legyen a vezető vagy a vezető által kijelölt személy és a rendszertulajdonos jóváhagyására. A Beszállító felelőssége annak biztosítása, hogy a Citi-adatokhoz hozzáféréssel rendelkező személyzeti tagok a szükséges ismeretek elve alapján kapjanak hozzáférést.
3. Annak megkövetelése, hogy egyéni felhasználónak ne lehessen kiadni különböző jogosultságok/beosztások kombinációját, ha ez érdekellentétet eredményez, vagy ha sérti a felhasználók szétválasztásának (maker-checker) szabályait.
4. Monitorozási folyamat, mely felügyeli és kezeli a rendszer egyes felhasználóinak megadott/azoktól visszavont hozzáférési jogokat.
5. A hozzáférési kérelmek nem alapulhatnak más felhasználó jogosultságainak tükrözésén vagy másolásán. A kérelmekben egyértelműen meg kell határozni a kért szerepköröket és jogosultságokat, azok üzleti indoklásával együtt, a jogosultságok fokozatos indokolatlan bővülésének megelőzése, valamint a legkisebb jogosultság elvének érvényesítése érdekében.

17.16 Felhasználók azonosítása és hitelesítése

A Beszállító minden ellenőrzött információs rendszerének el kell végeznie a platformhoz hozzáférni kívánó felhasználók vagy rendszerek azonosságának hitelesítését, mielőtt olyan munkameneteket vagy tranzakciókat indítana el, amely révén hozzá lehet férni Citi-információkhoz.

1. A felhasználókat egyedileg kell azonosítani vagy felhasználói azonosítóval kell hozzárendelni a technológiai platformhoz.
2. A felhasználókat jóváhagyott hitelesítési módszerrel kell hitelesíteni a technológiai platformon – az aktuális jóváhagyott módszerekkel kapcsolatban a Beszállítónak az elsődleges üzleti kapcsolattartójához (BAO) kell fordulnia.
3. A megosztott hitelesítési infrastruktúra (pl. Egyszeri bejelentkezés, Csökkentett bejelentkezés és egyéb megosztott hitelesítési szolgáltatások) használatának minden esetben meg kell felelnie a Citi hitelesítési követelményeinek. Az aktuális jóváhagyott módszerekkel kapcsolatban a Beszállítónak az üzleti tevékenységért felelős személyhez (BAO) kell fordulnia.
4. A felhasználó információs rendszerekben való hitelesítésére használt személyazonosság-ellenőrző adatokat (IVD) titkosítani kell az átvitel és a tárolás során. A titkosítási követelményeket lásd a 17.9. fejezetben.

5. A Beszállító munkatársai által a Citi rendszereihez való hozzáféréshez használt minden felhasználói fiókot egy egyedi, a Citi által hozzárendelt azonosítóhoz (pl. GEID) kell kapcsolni. Általános vagy megosztott felhasználói azonosítók természetes személyek számára nem használhatók, a nyomon követhetőség, az SoD érvényesítése és az auditálhatóság biztosítása érdekében.

17.17 Privilegizált hozzáférések azonosítása és ideiglenes privilegizált hozzáférés

A Beszállítónak nyilvántartást kell vezetnie valamennyi digitális identitásról, és azonosítania kell azokat, amelyek privilegizált hozzáféréssel rendelkeznek, illetve hozzáférnek olyan elektronikus adattárolókhoz (adatkészletekhez vagy az üzleti alkalmazásokat támogató adatbázisokhoz), amelyek Bizalmas PII vagy annál magasabb minőségű információkat tartalmaznak. A Beszállítónak olyan ellenőrzéseket kell alkalmaznia, melyek védelmet nyújtanak ezen Azonosítók jogosulatlan használatával szemben. Ha egy munkavállaló hozzáférést igényel egy privilegizált azonosítóhoz vagy a fent említett elektronikus adattárakhoz, akkor a hozzáférést egy olyan ideiglenes hozzáférés-kezelési folyamaton keresztül kell biztosítani, amely:

1. Előírja, hogy a kérelmező az előzetesen jóváhagyott, engedélyezett felhasználókat tartalmazó listán legyen, vagy a használat idején engedéllyel rendelkezzen.
2. A hozzáférés engedélyezése előtt módosítással/problémával kapcsolatos szolgáltatási jegyben dokumentált indoklást követel.
3. Tartalmazza a hozzáféréssel végzett tevékenység független áttekintését.
4. Tartalmaz eljárást amivel az ideiglenes hozzáférés engedélyezett időtartamának lejártával a hozzáférés visszavonása vagy megszüntetése automatikusan kezdeményezhető.
5. Lehetővé teszi a működési környezetben való és megvalósítás utáni stabilizációs hozzáférés meghosszabbítását – például egy nagyobb frissítés vagy meghibásodás/javítás után – akár hét (7) naptári nappal.

17.18 Felhasználói hozzáférési jogosultságok felülvizsgálata

1. A Beszállítónak be kell vezetnie egy dokumentált eljárást a Citi-információk tárolására, feldolgozására, kezelésére és/vagy továbbítására használt ellenőrzött információs rendszerekhez való szükségtelen felhasználói jogosultságok felülvizsgálatára, ellenőrzésére és törlésére, amelyet legalább félévente el kell végeznie.
2. A felhasználók nem vizsgálhatják felül vagy hagyhatják jóvá saját jogosultságait vagy olyan személyek jogosultságait, akik a felülvizsgálati felelősségi kört számukra kiosztották.
3. Ha a Beszállító alkalmazottjának megváltozik a Citin belüli beosztása, akkor a Beszállítónak 14 naptári napja van a hozzáférés és a jogosultság felülvizsgálására, valamint a Citi-adatokhoz való hozzáférés eltávolítására, amennyiben arra az új beosztásban már nincs szükség.

17.19 Biztonságos bejelentkezési eljárások

1. A letiltott felhasználói bejelentkezési azonosítók tiltásának feloldását az ipari szabványoknak megfelelő helyreállítási szolgáltatáson vagy más jóváhagyott funkción keresztül kell elvégezni. Ha az operációs rendszer vagy az alkalmazás támogatja, akkor értesítésszalagnak kell megjelenítenie minden olyan hálózati belépési ponton, ahova a felhasználó először jelentkezik be, vagy ahol először hitelesíti a rendszer.

17.20 Jelszókezelő rendszer

1. A statikus felhasználói jelszavakat minden esetben tilos nem titkosított szöveggként megjeleníteni a képernyőn. A jelszó láthatóságának be- és kikapcsolását lehetővé tevő funkció mentesül e követelmény alól, feltéve, hogy:
 - (1) A jelszó bevitele alapértelmezés szerint maszkolt,
 - (2) A jelszó megjelenítése kizárólag a felhasználó kifejezett műveletével engedélyezhető, (3) A jelszó ismét maszkolásra kerül legfeljebb 15 másodperccel azután, hogy a felhasználó befejezte a megjelenítést kezdeményező műveletet.
2. A privilegizált Funkcionális azonosítókhoz tartozó jelszavakat tilos nem titkosított szöveggel kódolni.
3. A statikus jelszavaknak legalább tíz (10) karakterből kell állniuk, betűket és számokat egyaránt kell tartalmazniuk, valamint különbséget kell tenniük a kis- és nagybetűk között. A statikus jelszavak kis- és nagybetű-érzékenységét minden hitelesítési ponton ellenőrizni kell. A 2026. augusztus 31. után bevezetett alkalmazásokban a funkcionális azonosítókhoz (FID) tartozó statikus jelszavaknak legalább 15 karakterből kell állniuk.
4. PIN-kódokat kizárólag akkor lehet egyedüli hitelesítési módszerként használni az információs rendszerekhez való hozzáféréshez, ha a PIN-kódokra az adott eszköz fizikai korlátai miatt van szükség (pl. számbillentyűzet, telefon, intelligens kártya).
5. Minden statikus jelszót legalább 90 naptári naponként meg kell változtatni.
6. Valamennyi statikus jelszót legfeljebb hat (6) egymást követő sikertelen bejelentkezési kísérlet, illetve hat (6) egymást követő sikertelen jelszó-visszaállítási kísérlet után zárolni kell. A jelszavak letiltását egy azonosító-rendszergazda funkción keresztül kell feloldani, vagy a letiltásnak automatikusan kell feloldódnia legalább 30 perc elteltével.
7. Minden hitelesítési rendszernek alkalmaznia kell egy bejelentkezési inaktivitást/használat hiányát szabályozó funkciót, amely nem engedélyezheti azt 100 napnál tovább. Ha technikailag megvalósítható, akkor a letiltott bejelentkezési azonosítókat a felhasználó vagy egy másik meghatalmazott funkció aktiválhatja újra.
8. A hitelesítési eljárásnak biztosítania kell, hogy legalább hat (6) jelszócsere során ne kerüljön ismételt beállításra ugyanaz a jelszó.

17.21 Rendszereszközök használata

A Beszállítónak gondoskodnia kell arról, hogy a rendszer- és alkalmazásvezérlőket felülbírálni képes segédprogramok (pl. perifériás eszközökről történő rendszerindítás) használata korlátozott és ellenőrzött legyen.

17.22 Munkamenet lejárata

1. A Citi-információk tárolására, feldolgozására és/vagy továbbítására használt Ellenőrzött információs rendszerek összes felhasználójánál el kell végezni a bejelentkezést és az újbóli hitelesítést.
2. A felhasználókat 30 percet nem meghaladó inaktivitás után újra hitelesíteni kell. Az aktivitás magában foglalja a végponton (egérrel, billentyűzetten, érintőképernyőn stb.) végzett minden bevitelt. Ha a kényszerítést jelszóval védett képernyővédő biztosítja, akkor az alkalmazásba való bejelentkezés/egyszeri bejelentkezés kényszerítésére nincs szükség.

17.23 Felhasználói hozzáférés megszüntetése

1. Elbocsátás vagy felmondás esetén a Bizalmas vagy magasabb besorolású Citi-adatokhoz való hozzáférést biztosító felhasználói hozzáférést vagy jogosultságokat (beleértve az asztali számítógépen/Active Directoryn használt felhasználói bejelentkezési adatokat, az Egyszeri bejelentkezési adatokat (SSO), az e-mailt, az Egyszeri jelszavakat (OTP) generáló tokeneket és a távoli hozzáférést) haladéktalanul el kell távolítani.
2. Ha egy munkavállaló hozzáféréssel rendelkezik a Citi tulajdonában lévő és irányítása alatt álló rendszerekhez, akkor az adott munkavállaló beosztásának változásáról vagy a munkavállaló felmondásáról/elbocsátásáról azonnal értesíteni kell a Citi üzleti ügyfélkapcsolati felelőst, a BAO-t vagy a BAO-támogatást, hogy a Citi üzleti ügyfélkapcsolati felelős elindíthassa a távozó munkavállaló hozzáféréseinek eltávolítását a felmondási időszak lejártá előtt.
3. A Beszállítónak dokumentált eljárással kell rendelkeznie az összes eszközön, hogy a hozzáférést a 17.23.2. fejezetben meghatározott időkereteken belül visszavonja, ha egy munkavállaló vagy nem munkavállalónak minősülő személy felmond vagy elbocsátják.
4. Ha a Beszállító a 17.23.1.–17.23.3. fejezetekkel kapcsolatban bármilyen rendellenességet észlel, akkor köteles haladéktalanul értesíteni a Citi üzleti ügyfélkapcsolati felelőst, a BAO-t vagy a BAO-támogatást, a megfelelő indoklással és intézkedésekkel.

17.24 Távoli hozzáférés

A Beszállítónak távoli hozzáférés-szabályozással kell rendelkeznie azon hálózatok védelme érdekében, melyek képesek a Bizalmas vagy magasabb besorolású Citi-adatokat tárolni, feldolgozni vagy továbbítani. Ezek közé tartozhatnak többek között a következők:

1. A Citi-információk tárolására, feldolgozására, kezelésére és/vagy továbbítására használt Információs rendszerekhez való távoli hozzáférés védelme a jogosulatlan használattal szemben.
2. Minden olyan, a Beszállító által kezelt laptop és a Beszállító által kezelt asztali számítógép esetén, amelyet Citi-információk tárolására, feldolgozására és/vagy továbbítására használnak, és amellyel távoli hozzáférést kezdeményeznek úgy, hogy azon Bizalmas vagy magasabb besorolású Citi-

információkat tárolnak/dolgoznak fel, az iparági szabványoknak megfelelő titkosítási eszközzel végzett titkosítást kell alkalmazni.

3. Távoli kapcsolatokat kizárólag jóváhagyott, többfaktoros hitelesítést (MFA) használó távoli hozzáférési megoldásokon keresztül szabad létrehozni.
4. A Beszállító által kezelt gépeken aktív személyes tűzfalat kell használni, amikor közvetlenül (azaz nem a Beszállító által kezelt tűzfalon vagy proxyn keresztül) csatlakoznak az internethez.
5. A Beszállító által kezelt eszközöknek rendszeresen kapcsolódniuk kell a Beszállító hálózatára, hogy az eszközök megkaphassák és telepíthessék a rendszeres szoftver- és vírusirtó-frissítéseket, ami követelmény a hálózathoz való teljes hozzáféréshez. Korlátozott hozzáférés engedélyezhető kifejezetten az eszköz frissítése céljából.
6. Ha nem a Beszállító tulajdonában vagy irányítása alatt lévő eszközökkel férnek hozzá Bizalmas vagy magasabb besorolású Citi-információkhoz, akkor olyan jóváhagyott megoldást kell alkalmazni, amely letiltja a helyi gépre való letöltés lehetőségét. A következő ellenőrzési eszközöknek kell érvényben lenni:
 - a) A Citi-adatokat nem lehet letölteni olyan eszközre, amely nem a vállalat által felügyelt megoldás része.
 - b) A Beszállítónak biztosítania kell az ilyen hozzáférés védelmét tokenalapú vagy tanúsítványalapú hitelesítéssel, standard távoli hozzáférési technológiák (pl. virtuális asztali interfész (VDI), Horizon stb.) felhasználásával.
 - c) A Terminal Services, a VMware Horizon és más hasonló távoli hozzáférési megoldások konfigurálása során le kell tiltani a megosztott vágólapot, valamint a Blast és a PCoIP protokollokon keresztüli meghajtó-csatlakoztatás funkciót, és le kell tiltani az RDP és az SSH protokollokat.
7. Ha a többfaktoros hitelesítéshez (MFA) szoftveres tokeneket használnak, például mobil eszközön található szoftveralkalmazás elérésére, akkor a szoftveres token hitelesítő szoftvernek hitelesítenie kell a felhasználót (pl. jelszóval, biometrikus adatokkal stb.), és meg kell akadályoznia annak használatát, ha a mobiltelefont függetleníti vagy rootolják (a mobil eszköz forgalmazója által hitelesített és biztosított operációs rendszertől eltérő operációs rendszer használatával).
8. A Beszállító Személyzetének minden olyan tagjánál, ideértve többek között azokat az állandó/ideiglenes alkalmazottakat, vállalkozókat és alvállalkozókat, akiknek speciális, privilegizált és/vagy rendszergazda szintű hozzáférésre van szükségük a rendszerekhez, adattárakhoz, alkalmazásokhoz és/vagy infrastruktúrához, ideértve többek között a rendszergazdákat, az adatbázis-adminisztrátorokat, a hozzáférés-felügyeleti adminisztrátorokat, a tűzfal-adminisztrátorokat, a webhely-adminisztrátorokat stb., aki közvetlenül vagy közvetve kapcsolódik a Citi számára nyújtott Szolgáltatásokhoz, kizárólag MFA-hitelesítést lehet alkalmazni, és az ilyen hozzáférést a Beszállítónak függetlenül kell naplózni és felügyelni gyanús tevékenység és/vagy jogosulatlan hozzáférés tekintetében, a Citi fent említett, Beszállítókra vonatkozó Követelményeivel összhangban.

9. A személyes tulajdonban lévő eszközök és a harmadik fél tulajdonában lévő eszközök esetében a Beszállítónak rendelkeznie kell olyan hatékony megoldással, mellyel a hálózatra való bejelentkezés engedélyezése előtt biztosítható, hogy az ilyen eszközök rendelkeznek a megfelelő operációsrendszer-verzióval, javítási szinttel, vírusirtó és kártevőirtó megoldásokkal.
10. A Beszállítónak gondoskodnia kell arról, hogy személyzetének minden tagja:
 - a) Privát, kizárólag adott célra használt távoli munkaterületet tartson fenn, amelyen nem találhatók hangasszisztens eszközök (pl. Siri, Alexa), videórögzítő eszközök és/vagy egyéb olyan eszközök, amelyek fénykép, videó vagy hang hallgatására/felvételére szolgálnak. Jogosulatlan személyzet nem kaphat engedélyt a távoli számítástechnikai rendszerek képernyőjén megjelenő adatok, rendszerek vagy alkalmazások megtekintésére.
 - b) Zárolja a számítástechnikai eszközt, amikor azt felügyelet nélkül hagyja, hogy biztosítsa a képernyőhöz való jogosulatlan hozzáférés kockázatának megfelelő csökkentését.

17.25 Tiszta asztal szabályzat

A Beszállító alkalmazottai kötelesek védeni a Citi-információkat azok minden formájában, beleértve a munkaterületükön használt vagy tárolt fizikai információkat is. A Beszállítók kötelesek e követelményt minden dolgozójukkal közölni legalább évente egyszer, az információbiztonsági képzés keretében vagy egyéb csatornán keresztül.

17.26 Tűzvédelem

1. A Beszállítónak meg kell felelnie a fizikai biztonságra és a biztonságos munkakörnyezet kialakítására vonatkozó hatályos jogi és szabályozási követelményeknek, beleértve a helyi tűzvédelmi előírásokat.
2. A Beszállító köteles tűzjelzőt, tűzriasztó és tűzoltó rendszert alkalmazni. A rendszer(ek)e)t félévente ellenőrizni és évente tesztelni kell.

17.27 Fizikai biztonság

1. A Citi-információkat biztonságos területen kell tárolni, ahol csak a jogosult alkalmazottak férhetnek hozzá.
2. A Beszállítónak dokumentált és auditálható fizikai beléptető rendszerrel kell rendelkeznie.
3. A Beszállítónak a környezetnek és a nyújtott szolgáltatásoknak megfelelően biztonsági riasztó/behatólásjelző rendszerek kombinációját kell alkalmaznia, amely magában foglalja a harmadik fél által felügyelt biztonsági riasztást, biztonsági őrséget és videofelügyeletet.
4. A Beszállítónak rendelkeznie kell dokumentált látogatói szabályzattal, amelynek tartalmaznia kell azt a követelményt, hogy érkezéskor, be- és kijelentkezéskor minden látogatónak igazolnia kell a személyazonosságát.

17.28 Működési biztonsági eljárások és felelősség

1. A Beszállító változáskezelési folyamatának ki kell terjednie a fő ellenőrzési pontokra a változások regisztrálása, felülvizsgálata, tesztelése, jóváhagyása, végrehajtása és lezárása során. A Beszállítónak továbbá rendelkeznie kell

egy vészhelyzeti folyamattal is a változásokra vonatkozóan, mely előírja a kötelező jóváhagyások hierarchiájának beépítésével kapcsolatban felsorolt összes szakaszt.

2. A Beszállítónak rendelkeznie kell egy auditálható kapacitáskezelési folyamattal, melynek magában kell foglalnia többek között (de nem kizárólagosan) a következőket: rendelkezésre állási, kapacitás- és teljesítménymérők/mutatók; üzleti hatásvizsgálat; proaktív nyomon követés; a teljesítmény- és kapacitásproblémák kivizsgálása és kezelése.
3. Adott esetben a Beszállítónak gondoskodnia kell arról, hogy a laboratóriumi, a fejlesztési, a tesztelési és a gyártási környezetek mindegyike fizikailag és/vagy logikailag elkülönüljön egymástól.

17.29 Szoftverfejlesztési követelmények

Azokra a Beszállítókra vonatkoznak, amelyek kizárólag a Citi számára fejlesztett szoftvert szállítanak. A Beszállítónak meg kell felelniük ezeknek a követelményeknek, vagy igazolniuk kell, hogy olyan dokumentált és jóváhagyott szoftverfejlesztési életciklus-folyamattal („SDLC”) rendelkeznek, amely azonos szintű minőséget biztosító, egyenértékű megközelítést alkalmaz.

17.30 Projektindítás és tervezés

A Beszállítónak a megoldás hatókörét és célkitűzéseit a Citi követelményeivel és a szerződéses kötelezettségekkel összhangban kell meghatároznia. Ezek közé tartoznak a következők:

1. A funkcionális és nem funkcionális követelmények dokumentálása;
2. A szükséges erőforrások és a megvalósítás ütemezésének becslése; és
3. Valamennyi harmadik féltől származó komponens vagy szoftverfüggőség azonosítása.

A megfelelő tevékenységeket – beleértve a biztonsági kockázatértékeléseket is – a projekt kezdetétől meg kell indítani. A szerepköröket, felelősségi köröket és jóváhagyási pontokat egyértelműen meg kell határozni és kommunikálni kell.

Minden környezetet fejlesztői (DEV), tesztelési (TEST) vagy éles (PROD) környezetként kell besorolni, és ezeket a szoftver teljes életciklusa során szigorúan el kell különíteni. A környezet besorolása határozza meg az alkalmazható hozzáférési jogosultságokat, valamint az adott környezetben kezelhető adatok típusát. A Beszállítónak a hozzáféréseket a környezet besorolásának megfelelően kell korlátoznia, és a telepítéseket az SDLC megfelelő szakaszának lezárásához kell igazítani, hogy megelőzze a jogosulatlan hozzáférést és az adatok illetéktelen hozzáférhetővé válását.

17.31 Tervezés

Beszállítónak olyan tervezési megközelítést kell dokumentálnia, amely biztosítja, hogy a szállított megoldás valamennyi meghatározott követelménynek megfeleljen („Tesztterv”). A Teszttervnek legalább az alábbiakat kell tartalmaznia és ismertetnie:

1. 1.A fejlesztőcsapat által végrehajtandó valamennyi tesztet – beleértve az egységteszteket, a funkcionális és nem funkcionális teszteket, valamint a teljesítményvizsgálatokat –, biztosítva azok a követelmények szerinti visszakövethetőségét;
2. 2.Azon jóváhagyásra jogosult személy(ek) megjelölését, akik igazolják a sikeres végrehajtást;

3. 3.A biztonsági tesztelés követelményeit, például a sérülékenységvizsgálatokat és a fenyegetésmodellezést; valamint
4. 4.A tesztelési környezetet, az alkalmazott módszertant, a folyamatot és a telepítési előléptetési útvonalat.

El kell készíteni egy kiadási stratégiát, amely meghatározza a TEST és PROD környezetekbe történő kiadás előfeltételeit és folyamatát, beleértve a kiadásra való megfelelőség kritériumait, a kiadások tartalmát, valamint a kiadások ütemezését a projekt teljes életciklusa során.

Amennyiben azt a szerződés előírja, a szoftverkiadásokat a Citi által jóváhagyott formátumban, a Citi által jóváhagyott eszközök és munkafolyamatok alkalmazásával kell csomagolni.

17.32 Tesztelés

A tesztelést ellenőrzött környezetben kell megtervezni és végrehajtani, igazolva, hogy a megoldás megfelel a meghatározott követelményeknek és elfogadási kritériumoknak. A tesztesetek és a követelmények, valamint a forráskód-módosítások közötti visszakövethetőséget biztosítani kell.

A Beszállítónak jelentést kell készítenie, amely összefoglalja a sikeres/sikertelen tesztek eredményeit, a fejlesztés során elvégzett további teszteket, valamint az el nem végzett teszteket és azok indokait („Tesztzáró jelentés”). A feltárt hibákat, a későbbi kiadásra halasztott funkciókat, valamint a még nem megoldott problémákra vonatkozó kockázatcsökkentő intézkedési terveket dokumentálni kell.

A Citi kérésére a Beszállítónak biztosítania kell az alábbiakat:

1. Részletes teszterv;
2. A tesztelés befejezésének igazolása és az eredmények Tesztzáró jelentésben történő dokumentálása; valamint
3. A teszteredmények visszakövethetősége a követelményekhez és a forráskód-módosításokhoz.

17.33 Telepítés

A telepítés előtt a Beszállítónak valamennyi előírt biztonsági vizsgálatot el kell végeznie, beleértve a sérülékenységvizsgálatokat és a fenyegetésmodellezést is. A kiadási folyamatnak dokumentált változásnyilvántartásokra, visszaállítási stratégiákra és a szükséges jóváhagyásokra kell épülnie. A bevezetési terveknek és a telepítési üzemeltetési eljárásrendeknek tartalmazniuk kell a monitorozási és eskalációs eljárásokat.

Az üzembe helyezést követően a Beszállítónak véglegesítenie kell a rendszerazonosítókat, és frissítenie kell minden kapcsolódó dokumentumot, hogy a rendszer készen álljon az audit lefolytatására.

17.34 Biztonság

1. Az SDLC tervezési szakaszában, a forráskód elkészítése előtt strukturált értékelést kell végezni a lehetséges biztonsági kockázatok, sérülékenységek és architekturális gyengeségek azonosítása és kezelése érdekében („Biztonsági tervfelülvizsgálat”). A Biztonsági tervfelülvizsgálatot az SDLC részévé kell tenni, és az OWASP-hoz hasonló iparági szabványokkal összhangban álló megelőző és felderítő kontrollokat kell tartalmaznia.

2. A biztonságos kódolási gyakorlatok alkalmazását biztosítani kell.
3. A Beszállítónak információbiztonsági ellenőrzésekkel kell kiegészítenie saját eljárásait és folyamatait az alkalmazások, termékek és szolgáltatások kiválasztására, fejlesztésére és bevezetésére vonatkozóan.
4. A Beszállítónak biztonságos buildfolyamattal kell rendelkeznie minden olyan rendszerre vonatkozóan, amelyben Citi-információkat tárolnak, dolgoznak fel és/vagy továbbítanak, továbbá minden rendszerhez biztonságos rendszerképet vagy sablont kell fenntartania.

17.35 Rosszindulatú szoftver elleni védelem

A Beszállítónak gondoskodnia kell arról, hogy sor kerüljön a kártékony programok (pl. vírusok, férgek, trójai falovak, reklámprogramok, kémprogramok, zsarolóvírusok és más hasonló kibertámadások, amelyek során adatok kompromittálódhatnak) behatolását akadályozó és feltáró ellenőrzések alkalmazására. A Beszállító köteles:

1. Vírusirtó és kémprogram-eltávolító technológiákat alkalmazni, frissíteni és fenntartani minden olyan személyi számítógépen, helyi hálózati (LAN) szerveren, e-mail-szerveren és más eszközön, amelyet Citi-adatok tárolására, feldolgozására és/vagy továbbítására használnak.
2. Biztonsági beállításokat alkalmazni, hogy megakadályozza a vírusirtó-/kémprogram-eltávolító eszközök, illetve az ütemezett vizsgálatok végfelhasználók általi kikapcsolását.
3. Központilag vezérelt, automatikus eljárásokat bevezetni a vírusirtó és a kémprogram-eltávolító szoftver konfigurálásához és frissítéséhez.
4. Gondoskodni a nem megfelelő, elavult vírusirtó-aláírásokkal vagy keresőmotorokkal rendelkező számítógépek azonosítására és kezelésére szolgáló folyamatok bevezetéséről.
5. Ellenőrizni a hozzáférést azokhoz a kommunikációs portokhoz/interfészekhez, amelyek lehetővé teszik a külső eszközökhöz, többek között, de nem kizárólagosan az adathordozókhoz való csatlakozást.

17.36 Mobil kód elleni ellenőrzések

A Beszállító köteles biztosítani a mobil kóddal kapcsolatos biztonságos gyakorlatokra vonatkozó ellenőrzések bevezetését. Amennyiben a mobil kód használata engedélyezett, a konfigurációnak legalább meg kell felelnie valamennyi vonatkozó iparági szabványnak és a Cítivel szembeni szerződéses kötelezettségnek. A Beszállítónak biztosítania kell továbbá, hogy az engedélyezett mobil kód egy egyértelműen meghatározott és dokumentált biztonsági szabályzatnak megfelelően működjön, valamint meg kell akadályoznia a jogosulatlan mobil kód végrehajtását.

Olyan mobil kódok esetében, amelyek hatást gyakorolhatnak az alapul szolgáló operációs rendszerre vagy platformra (azaz „tesztkörnyezeten” kívüli), a Beszállító köteles biztosítani a következőket:

1. A Beszállító által közzétett mobil kódot egy, a Citi által jóváhagyott Hitelesítésszolgáltató írja alá, és a hitelesítési tanúsítvány életciklusát – a lejáratával vagy a frissítéssel kapcsolatos intézkedések végrehajtása érdekében – a Beszállító kezelje.
2. A lejárt tanúsítvánnyal rendelkező aláírt mobil kódot eltávolítsa a rendszerből.

17.37 Eseménynaplózás

A Beszállítónak gondoskodnia kell arról, hogy a Citi-információk eléréséhez, tárolásához, feldolgozásához, kezeléséhez és/vagy továbbításához használt összes ellenőrzött információs rendszer rendelkezzen infrastruktúra- vagy alkalmazásszintű ellenőrzési nyomvonallal, a következő elemek naplózásához:

1. A kapcsolódó platformra vonatkozó, az infrastrukturális biztonság szempontjából releváns tevékenységek
2. A tűzfal vagy IDS/IPS rendszer által generált biztonsági eseményekhez köthető rendszerriasztások
3. A rendszerbiztonságot érő támadási kísérletek (pl. sikertelen bejelentkezési kísérletek)
4. Jogosulatlan kísérletek erőforrások (szoftverek, adatok, folyamatok stb.) elérésére
5. Rendszergazda által végzett műveletek
6. A felhasználtól vagy más rendszertől származó konkrét információk fogadásával kapcsolatos információk
7. Minden jelentős esemény, amely pénzügyi tranzakciókkal és Citi-információkkal kapcsolatos, különös tekintettel a következőkre:
 - a. A pénzügyi tranzakciók frissítése
 - b. Bizalmas vagy érzékeny személyes adatok (PII) módosításai
 - c. A korlátozott adatok frissítése
 - d. A hitelesítési adatok frissítése
8. Minden létrejött munkamenet
9. A Citihez fűződő alkalmazások (webhelyek és mobilalkalmazások) esetén a munkamenet elemeit, mint amilyen az egyéni eszközazonosító, kötelező rögzíteni – amikor az technikailag lehetséges – és naplózni a csalásokkal kapcsolatos vizsgálatok segítése érdekében. Ezeknek az elemeknek legalább az IP-címeket tartalmazniuk kell. Ezeket az elemeket rögzíteni kell a Citi-tranzakcióknál és a Citi-számlanyitási tevékenységnél. Az információkat rögzíteni kell, hogy a munkamenet-objektumok összekapcsolhatók legyenek a tranzakciókkal vagy számlanyitási folyamatokkal.
10. A letagadhatóság elkerülése érdekében az ellenőrzési nyomvonalaknak dokumentálniuk kell az adott tevékenységek adott személyhez való hozzárendelését.
11. A jelentős információbiztonsági adminisztrációs (ISA) eseményeket naplózni kell, különös tekintettel a következő elemekre:
 - a) Felhasználó létrehozása

- b) Felhasználók hozzáférési jogosultságainak módosítása
- c) Profilok törlése, létrehozása és módosítása az ellenőrzött információs rendszeren belül
- d) Jelszó-visszaállítások
- e) A rendszer biztonsági konfigurációjában végzett módosítások
- f) A privilegizált funkcionális azonosítók összes interaktív tevékenysége
- g) A biztonsági naplónak a naplót generáló rendszertől függetlenül legalább a következő információkat tartalmazniuk kell, kivéve, ha ez műszakilag nem kivitelezhető:
 - I. Az esemény dátuma és ideje (UTC formátumú idő)
 - II. A műveletet végrehajtó személy felhasználói azonosítója
 - III. Az esemény típusa
 - IV. Az érintett eszköz vagy erőforrás neve
 - V. A hozzáférés típusa (törlés, módosítás stb.)
 - VI. Az esemény sikeressége vagy sikertelensége
 - VII. A forrás (terminál, port, hely, IP-cím, hoszt neve stb.).

17.38 Naplóinformációk védelme

A Beszállító köteles biztosítani a hozzáférés ellenőrzését, ezáltal megőrizve az ellenőrzési nyomvonalak integritását az indítás, leállítás, tárolás és átvitel során.

1. A naplófájlok jogosulatlan módosításának megakadályozása érdekében a Beszállító köteles biztosítani, hogy a naplókat ne írassák felül vagy módosíthassák azok a rendszerfelhasználók, akiknek a tevékenységét nyomon követik.
2. A Beszállítónak a Citi rendelkezésére kell bocsátania egy naplóadat-megőrzési eljárást, amely meghatározza az adatok kezelésének módját, és tartalmazza az alkalmazandó jogszabályi és szabályozási követelményeknek való megfelelést biztosító intézkedéseket.
3. Egy szervezeten vagy biztonsági területen belüli összes releváns információfeldolgozó rendszer óráit szinkronizálni kell egy pontos időforrással.

17.39 A rendszerhasználat megfigyelése

A Beszállítók kötelesek biztosítani a következő események – közvetlen vagy automatizált felülvizsgálati folyamat révén való – rögzítését, naplózását és felülvizsgálatát:

1. A tűzfal vagy a behatolásészlelő rendszer (IDS)/behatolásmegelőző rendszer (IPS) által generált biztonsági eseményekhez kapcsolódó összes rendszerriasztás.
2. A biztonságos standard kiépítésben meghatározott kritikus erőforrásokat érintő összes frissítés.
3. Bizalmas PII vagy magasabb besorolású információ elérésére alkalmas bármely azonosító (funkcionális, privilegizált, rendszerszintű, ideiglenes stb.) által végzett interaktív tevékenység.
4. A fenti „Eseménynaplózás” című részben felsorolt jelentős ISA-események a következő kivétellel:
 - a) Jogosultságok eltávolítása olyan felhasználónál, szerepkörnél vagy profilnál, ahol az információbiztonsági adminisztrációs tevékenységet

olyan automatizált munkafolyamat/teljesítési rendszer hajtja végre, amely végpontok közötti integritás-ellenőrzéssel rendelkezik.

17.40 Naplókorreláció és felülvizsgálat

1. Ha egy naplózott esemény riasztást vált ki, és az eseményt felülvizsgálják, a Beszállítónak utókövetési intézkedéseket kell kezdeményeznie, valamint vizsgálatot kell indítania, amennyiben arra utaló jel merül fel, hogy potenciálisan káros információbiztonsági incidens történt.
2. A Beszállító köteles biztosítani, hogy az auditnaplókat központi naplókezelő rendszerben, például Biztonsági információ- és eseménykezelő (SIEM) rendszerben vagy naplóelemző eszközben összesítsék naplókorrelációs elemzés és áttekintés céljából.
3. A Beszállítóknak rendszeresen el kell végezniük a SIEM-rendszer vagy naplóelemző eszköz felülvizsgálatát és konfigurálását a káresemények beazonosításának javítása érdekében.

17.41 Operációs szoftverek ellenőrzése

A Beszállító köteles biztosítani, hogy kizárólag olyan operációs rendszerek és szoftverek legyenek használatban, melyeket iparági szinten elfogadott kereskedelmi szolgáltató folyamatosan támogat, és azokhoz aktívan megfelelő javítócsomagokat és konfigurációs frissítéseket bocsát ki a biztonsági problémák kiküszöbölésére.

A Beszállító köteles biztosítani, hogy bevezetésre kerüljön egy a jóváhagyott biztonsági javítások és konfigurációk alkalmazásának határidejét megszabó dokumentált eljárás.

A Beszállító és a Citi közötti esetleges külön karbantartási megállapodástól függetlenül a Beszállítónak biztosítania kell, hogy a Citi számára fejlesztett, licencszerződés hatálya alá tartozó szoftver ne tegye lehetővé ismert sérülékenységeket tartalmazó, már nem támogatott szoftververziók használatát, valamint hogy az ilyen szoftvereket az előírásoknak megfelelően, kellő időben frissítsék és lássák el biztonsági javításokkal.

A Citi-információk feldolgozására használt alkalmazásszoftvereket megbízható Beszállítótól kell beszerezni, és azoknak megfelelő licenccel, nyilvántartással és támogatással kell rendelkezniük.

17.42 Sebezhetőségek és fenyegetések kezelése

1. A Beszállító köteles bevezetni egy sebezhetőség- és fenyegetéskezelési eljárást, amely átfogóan tárgyalja és/vagy tartalmazza a következők mindegyikét:
 - a. Eszközök és eljárások a sebezhetőségek felderítésére és kezelésére az összes olyan eszközben, amely felhasználható a Citi Bizalmas vagy érzékenyebb adatainak feldolgozására, tárolására, elérésére vagy továbbítására.
 - b. Előírás, hogy a sebezhetőségi vizsgálatokat legalább hetente el kell végezni iparágilag elismert sebezhetőséget vizsgáló eszközök és jelentési módszertan alkalmazásával.

- c. A sebezhetőségek rangsorolása a „Közös sebezhetőségi pontozási rendszer (CVSS)” (lásd: <https://www.first.org/cvss>) legfrissebb verziója szerint, a súlyosságon alapuló orvoslási ütemtervekkel.
- d. Arra vonatkozó követelmény, hogy a biztonságirés-javításokat leteszteljék a teljes éles üzembe helyezés előtt.
- e. Dokumentált és megismételhető működési folyamat a kritikus biztonsági rések orvoslásának felgyorsítására.
- f. A Beszállítónak az eszközöket teljes támogatott életciklusuk során nyomon kell követnie annak érdekében, hogy felkészülhessen az életciklus végére (EOL) vagy a gyártói támogatás megszűnésére (EOVS), és olyan folyamatokkal kell rendelkeznie, amelyek biztosítják ezen eszközök proaktív frissítését vagy cseréjét.
- g. Az információgyűjtés, sebezhetőségi vizsgálatok vagy penetrációs tesztelés során azonosított, kritikus CVSS-pontszámú sebezhetőségeket kiemelt prioritással kell kezelni, és a kockázat mértékével arányos, egyértelműen meghatározott határidőn belül meg kell szüntetni.

17.43 Harmadik fél által szolgáltatott alkalmazások

Ha a Beszállító Bizalmas vagy érzékenyebb besorolású Citi-adatokat tart fenn vagy tárol egy webhelyen vagy interneten elérhető rendszeren vagy egy Citi márkánévvel ellátott webhelyen, akkor a Citit érintő termékekkel vagy szolgáltatásokkal kapcsolatos sebezhetőség vagy fenyegetés (ezek mindegyike „sebezhetőség”) elleni védelem érdekében a Beszállítónak meg kell felelnie a következő Követelményeknek:

1. A Beszállítónak ki kell jelölnie egy munkavállalót, aki a Citi információbiztonsággal kapcsolatos megkereséseire válaszol.
2. Az iparág által elismert bevált gyakorlatok kihasználása a számítógépes biztonsági sebezhetőségi információk jó hírű forrásainak legalább heti rendszerességgel történő figyelemmel kísérésére; ilyenek a FIRST, a CERT/CC, a CISA Ismert kihasznált sebezhetőségek katalógusa és a forgalmazói levelezőlisták. Ezenfelül megfelelő intézkedések a releváns szervizcsomagok, javítások, frissítések és megoldások beszerzésére, alapos tesztelésére, alkalmazására és a Citi számára történő biztosítására.
3. Legalább negyedévente felül kell vizsgálnia információbiztonsági intézkedéseinek megvalósítását hálózati, rendszer- és alkalmazásszintű sebezhetőség vizsgáló eszközök és/vagy penetrációs tesztelés alkalmazásával.
4. Lehetővé tenni a Citi, vagy a Citi által jóváhagyott harmadik fél számára, hogy észszerű időintervallumokon belül sebezhetőségi, etikai feltöréssel járó vagy egyéb biztonsági értékelést végezzen, biztosítva, hogy a Beszállító eleget tesz-e a vonatkozó szerződésből és a jelen Követelményekből fakadó kötelezettségeinek. Az ellenőrzés kiterjedhet többek között a szabályzatok, folyamatok és eljárások felülvizsgálatára, a fizikai biztonsági intézkedések helyszíni értékelésére, a hálózat, a rendszer és az alkalmazások sebezhetőségi ellenőrzésére, valamint behatolási tesztekre, kereskedelmi forgalomban kapható eszközök és/vagy iparági szabványos gyakorlatok felhasználásával.

5. Minden olyan vállalkozónak, aki a Beszállítónak sebezhetőségértékelési szolgáltatásokat nyújt, szerepelnie kell a Citi által jóváhagyott sebezhetőségértékelési szolgáltatók listáján. Ha a Beszállító vállalkozókat vagy alvállalkozókat vesz igénybe a Szolgáltatások nyújtásához, akkor köteles saját költségén biztosítani, hogy a megkövetelt sebezhetőségi értékeléseket ugyanúgy időben végezzék el, mintha a Beszállító közvetlenül nyújtaná ezeket a Szolgáltatásokat; továbbá köteles biztosítani, hogy a Beszállító és a vállalkozó/alvállalkozó között, a Szolgáltatásra vonatkozóan létrejött megállapodás minden vállalkozóra vagy alvállalkozóra nézve kötelezővé tegye az ilyen értékelések elősegítését, kifejezetten előírva, hogy a Citi jogosult ilyen értékeléseket végrehajtani.
6. **Értesítés.**
- a) Ha a Beszállító egy a Citit érintő termékkel vagy szolgáltatással kapcsolatos sebezhetőséget azonosít, az azonosítást követő 24 órán belül köteles írásban értesíteni a Citit, és mellékelni az általa tett helyreállítási intézkedések leírását.
 - b) Ha a Beszállító egy, a Citit érintő termékkel vagy szolgáltatással kapcsolatos sebezhetőségről értesül megbízható folyamat-közzétételi csatornákon keresztül (a Nemzeti sebezhetőségi adatbázisban (NVD) közzétett sebezhetőség vagy külső biztonsági forgalmazóknak biztosított fenyegetési katalógus útján), akkor a Beszállító köteles a közzétételt követő 24 órán belül írásban értesíteni a Citit. Minden értesítésnek tartalmaznia kell információkat a sebezhetőségről, le kell írnia a rendszer funkcióját a Citihez kapcsolódó szolgáltatások szempontjából (azaz Citi-információkat tárol, szolgáltatások nyújtására használják, vagy mindkettő), azt, hogy a sebezhetőség távolról is kihasználható-e, valamint a Gyakori sebezhetőségek és kitétségek (CVE) pontszámot. A Beszállító köteles folyamatos tájékoztatást biztosítani a Citi számára a sebezhetőség elhárításáig. Ha a Citi azonosít egy sebezhetőséget, a Citi értesítheti erről a Beszállítót; a Beszállító ilyen esetben köteles a jelen fejezetnek megfelelően haladéktalanul orvosolni a sebezhetőséget.
7. **Kármentesítés.** A bejelentő fél az e fejezetben meghatározott minden egyes sebezhetőség esetében felméri az adott sebezhetőség kockázati szintjét és hatását a súlyosság és a Citit érintő kockázat alapján, továbbá kockázati prioritási szintet rendel hozzá az „A” Függelékben megadott közös sebezhetőségi pontozási rendszer (CVSS) alapján (lásd: <https://www.first.org/cvss>). A kockázati szint megállapítását és elfogadását követően a Beszállító köteles kijavítani minden azonosított közepes, magas vagy kritikus szintű sérülékenységet. Ahol ez lehetséges, az adott sebezhetőség javítását elérhetővé kell tenni a jelenleg telepített kiadáshoz tartozó biztonsági csomagban.

Ha a Beszállító nem tudja vagy nem szándékozik kiküszöbölni a sebezhetőséget a Citi elvárásainak megfelelően a megadott határidőn belül, akkor a Citi (a megszüntetett részre vonatkozóan) minden további felelősség vagy pénzügyi kötelezettség nélkül megszüntetheti a vonatkozó licencet, a Beszállító pedig köteles haladéktalanul visszatéríteni a Citi részére a kifizetett licencdíjak időarányos részét.

17.44 Kommunikációs biztonsággal kapcsolatos hálózatvédelmi intézkedések

1. A Citi információk elérésére, tárolására, kezelésére, feldolgozására és/vagy továbbítására használt beszállítói hálózatokat védeni kell a fenyegetésekkel szemben, és gondoskodni kell az információs rendszerek biztonságának fenntartásáról hálózati kényszerítési pontok használatával.
 - a. A Citi információkra vonatkozó besorolása szerint Bizalmas vagy magasabb szintű információkat tilos tartósan olyan rendszeren tárolni, amely internetkapcsolattal rendelkező demilitarizált övezetben található. Azok a hálózatok, amelyek olyan vezeték nélküli helyi hálózatok (WLAN-ok) vagy más olyan vezeték nélküli eszközmegoldások segítségével érnek el, tárolnak, kezelnek, dolgoznak fel és/vagy továbbítanak Citi-információkat, amelyek észszerű ellenőrzéseket (PEAP-TLS, EAP-TTLS stb.) tartalmaznak a jogosulatlan hozzáférések tiltására, csatlakoztathatók Citi-információkat tartalmazó hálózatokhoz.
 - b. A Beszállító globális hálózatahoz vezető összes külső IP-kapcsolatot a Beszállító által felügyelt tűzfalnak kell védenie.
 - c. Valós idejű behatolásérzékelő rendszert (IDS) és behatolásmegelőző rendszert (IPS) kell alkalmazni, amely felügyeli és védelmezi a Beszállító által a Citi-információk elérésére, kezelésére, tárolására, feldolgozására és/vagy továbbítására használt hálózathoz befutó valamennyi internetes kapcsolatot.
2. A Beszállító minden Citi márkával ellátott internetes alkalmazásnál köteles biztosítani a következőket:
 - a. A Beszállító webhelyein hosztolt szolgáltatásokat a Citi által jóváhagyott DDoS (elosztott szolgáltatásmegtagadásos támadások) elleni szolgáltatásokkal vagy a Citi által érvényesített más hasonló eszközökkel kell védeni.
 - b. A külső tűzfalakat alapértelmezett megtagadási szabállyal kell konfigurálni. A tűzfalszabályokat a legkisebb jogosultság elve alapján kell konfigurálni, és minden a tűzfal által megtagadott csatlakozási kísérletet (pl. eldobott csomagot) naplózni/rögzíteni kell.
 - c. A hálózati kommunikációs forgalmat alapértelmezés szerint le kell tiltani, és kivételek megadásával kell engedélyezni ellenőrzött interfészeken. A kivételeket szigorúan meghatározott forrásokra, célállomásokra vagy szolgáltatásokra kell korlátozni.
 - d. A webalkalmazások forgalmát megfelelő biztonsági kontrollokkal kell védeni és szűrni, például webalkalmazási tűzfal használatával.

17.45 Hálózatok elkülönítése

A Beszállító köteles biztosítani, hogy a Citi-információk eléréséhez, tárolásához, feldolgozásához, kezeléséhez és/vagy továbbításához használt, és az interneten keresztül elérhető összes Információs rendszerhez és alkalmazáshoz csak a Beszállító demilitarizált zónáján (DMZ) keresztül lehessen hozzáférni.

Vészhelyzet esetén a Beszállítónak képesnek kell lennie a hozzáférés szűrésére a hálózat egyes részei között a hálózati biztonsági események hatásának csökkentésére (pl. portszűrés vírus kitörése során).

A távoli elérésnél és a hoszt biztonsági rendszerében csoportalapú hozzáférés-szabályozást (pl. személyzet, alvállalkozók) kell alkalmazni a hálózati erőforrásokhoz való hozzáférés korlátozására a Beszállító hálózatán. A hoszt szintjén a hozzáférés-vezérlés csoportos vagy egyéni alapon történhet.

17.46 Berendezések hálózaton belüli azonosítása

A technológiai platformoknak az interakció információs biztonsági kockázati szintjének és egyéb mérséklésre irányuló ellenőrzéseknek megfelelően kell azonosítaniuk és hitelesíteniük a társközi technológiai platformokat.

1. Azokhoz a beszállítói hálózatokhoz, amelyeken Citi-információkat tárolnak, dolgoznak fel vagy továbbítanak, kizárólag olyan beszállítói eszközök (azaz hardverek, beleértve az asztali számítógépeket és a laptopokat is) férhetnek hozzá, amelyek megfelelnek ezeknek a követelményeknek, és amelyekre a Beszállító engedélyt adott.
2. A Citi hálózatához kizárólag olyan beszállítói eszközök (azaz hardverek, beleértve többek között, de nem kizárólagosan az asztali számítógépeket, laptopokat és a cserélhető adathordozókat) férhetnek hozzá, amelyek megfelelnek ezeknek a követelményeknek, és amelyekre a Citi engedélyt adott.

17.47 Biztonsági követelmények elemzése és specifikációja

A Beszállítónak különálló információbiztonsági eljárásokkal kell kiegészítenie saját eljárásait és folyamatait az alkalmazások, termékek és szolgáltatások kiválasztására, kifejlesztésére és bevezetésére vonatkozóan.

17.48 Online tranzakciók

1. Adott esetben a Beszállítónak rendelkeznie kell olyan információs rendszerekkel, amelyek dinamikus jelszavakat vagy digitális tanúsítványokat használnak a hitelesítő adatok érvényesítéséhez.
2. Minden végfelhasználói tanúsítványt 13 havonta legalább egyszer le kell cserélni.
3. Az olyan beszállítói alkalmazásnak, amely Citi-információkat tárol, dolgoz fel, kezel vagy ér el, Citi márkával ellátott internetes alkalmazásokért hosztként felel, vagy kapcsolódik a Citi hálózati erőforrásaihoz:
 - a. Az elért adatok/funkciók típusain alapuló hitelesítési módszert kell alkalmaznia;
 - b. Többtenyezős hitelesítési (MFA) megfelelőségértékelést kell végeznie, és szükség esetén alkalmaznia kell a javaslatokat;
 - c. El kell végeznie a gyanús tevékenységek megfigyelésének (SAM) kezdeti értékelését, és szükség esetén alkalmaznia kell a javaslatokat;

- d. Ezek mindegyike esetében a Beszállítónak az elsődleges üzleti kapcsolattartójához kell fordulnia a Citi aktuális követelményeivel kapcsolatban.

17.49 Változásellenőrzési eljárások

1. A Beszállító köteles gondoskodni arról, hogy a tűzfalak, Behatolásérzékelő rendszerek (IDS) és Behatolásmegelőző rendszerek (IPS) konfigurációs módosításai a Beszállító változáskezelési folyamatán keresztül kerüljenek megvalósításra.
2. A termeléshez ideiglenes azonosítókkal biztosított hozzáférést kötelező naplózni és felügyelni a környezetben végrehajtott változások nyomon követésére.
3. A Citi besorolása szerint Bizalmas vagy magasabb szintű ügyféladatokat tartalmazó, illetve „Magas” szintű „Integritás” vagy „Elérhetőség” információbiztonsági kockázati komponens értékkel bíró Ellenőrzött információs rendszerek esetén a Beszállító köteles felülvizsgálni a 17.32. (Eseménynaplózás) fejezet szerint rögzített naplókat. Az ilyen felülvizsgálatok alapulhatnak megfelelő kockázatalapú mintavételi módszeren.
4. A felülvizsgálatnak igazolnia kell, hogy az ideiglenes privilegizált hozzáféréssel megvalósított módosítások a tervek szerint történtek.
5. A Beszállító köteles dokumentálni minden változást, beleértve a felülvizsgálati folyamat bizonyítékainak tárolását is.

17.50 Adatszivárgás

A Beszállítónak rendelkeznie kell egy, az információk, többek között az alábbiak kiszivárgását megelőző dokumentált biztonságos kódolási normával:

1. Részletes rendszerinformációk (pl. szervertípus és -technológia).
2. Veremkivonatok és kivételi hibák, amelyek felfedik a könyvtárfa szerkezetét és az alapul szolgáló adatbázis típusát.

17.51 Tesztadatok

A Citi által Bizalmas vagy magasabb besorolással ellátott információkat a Beszállító nem használhatja fel vagy tárolhatja szoftveralkalmazás(ok) fejlesztési vagy tesztelési környezetekben vagy Laboratóriumokban, kivéve, ha az információk azonosításra alkalmas részeit eltávolították, maszkolták és/vagy titkosították iparági szabványoknak megfelelő eszközök és módszerek segítségével, úgy, hogy ezen adatok érzékeny jellege megszűnik; alternatív megoldásként a Beszállító köteles az éles rendszerre vonatkozó ellenőrzési eszközöket alkalmazni a fejlesztési vagy a tesztelési környezetekben.

17.52 Rendszer elfogadása

A Beszállítónak rendelkeznie kell olyan dokumentált projekthatóköri-kezelési és rendszerelfogadási folyamatokkal, amelyek megfelelnek a vonatkozó iparági szabványoknak.

17.53 Információbiztonsági hiányosságok jelentése

A Beszállítónak rendelkeznie kell olyan Eljárással, amely biztosítja a Citi információs eszközeit kompromittáló alkalmazás- és infrastruktúrabeli sebezhetőségek **Citi felé történő azonnali jelentését.**

17.54 Biztonsági incidensekkel kapcsolatos felelősségi körök és eljárások

1. A SIRT olyan biztonsági esemény, amely az alábbiak bármelyikének sérülését eredményezi, függetlenül attól, hogy a biztonsági incidens hogyan vagy hol következett be, illetve ki okozta azt:
 - A Citi adatainak bizalmassága, sértetlensége vagy rendelkezésre állása sérül.
 - Bármely olyan adat (beleértve a személyes adatokat is) bizalmassága, sértetlensége vagy rendelkezésre állása sérül, amely tekintetében a Citit szerződéses, jogszabályi vagy hatósági kötelezettségek terhelik.
 - A Citi azon információs rendszereinek sértetlensége vagy rendelkezésre állása sérül, amelyek Citi-adatokat tárolnak, dolgoznak fel vagy továbbítanak.
2. Jelen alkalmazásban a bizalmasság sérülése alatt azt kell érteni, hogy az adatokhoz jogosulatlan személy fér hozzá, vagy a Citi elveszíti az adatok feletti felügyeletet és ellenőrzést. Minden biztonsági incidenst haladéktalanul jelenteni kell.
3. Ha a Beszállítónál SIRT következik be, a Beszállítónak együtt kell működnie a Citivel a Citi incidenskezelési folyamatai alapján kért információk rendelkezésre bocsátásában, valamint az érintett adatok olyan módon történő elemzésében, amely lehetővé teszi a Citi számára a jogszabályi, hatósági és belső irányítási követelmények teljesítését. A Beszállítónak saját költségén meg kell tennie minden jogszabály, előírás vagy szabályozás által megkövetelt, illetve a Citi által kért értesítést, de kizárólag azt követően, hogy a Citi lehetőséget kapott a tervezett értesítési szöveg felülvizsgálatára és módosítására. A Beszállító ilyen értesítésekben nem nevezheti meg a Citit, kivéve, ha erre a Citi írásban kifejezetten felhatalmazást ad.

17.55 Adatszivárgás elleni védelem (DLP)

A Beszállító köteles adatszivárgás elleni védelmet szolgáló (DLP) szabályozásokat bevezetni, többek között a Bizalmas vagy magasabb szintű Citi-adatokhoz hozzáféréssel rendelkező alkalmazottakra kiható tartalom- és végpont-ellenőrzést.

A Beszállító köteles ellenőrzéseket alkalmazni azon esetek észlelésére és/vagy megakadályozására, amikor Bizalmas vagy magasabb besorolású Citi-adatokat mozgatnak át a hálózatról az alábbi csatornák segítségével:

- a. Titkosítatlan e-mailek
- b. Titkosított e-mail-csatolmányok
- c. Citi-adatok nyomtatása

- d. Citi-adatok hálózaton kívüli helyekre való továbbítása (például FTP segítségével)
- e. A bizalmas vagy magasabb szintű Citi adatok cserélhető adathordozókra, mint például USB-meghajtóra, cserélhető merevlemezekre, CD/DVD lemezre, vagy egyéb adattárolási képességgel rendelkező cserélhető eszközökre való másolása. Ezt a jogosultságot alapértelmezés szerint meg kell akadályozni.
- f. Az adatszivárgás elleni védelmet szolgáló (DLP) megoldásnak naplózni kell minden olyan eseményt, és riasztania kell a Beszállítót minden olyan eseményről, mely (akár sikeres, akár blokkolt) kísérletet jelenthet Bizalmas vagy magasabb besorolású Citi-adatok mozgatására, átvitelére vagy másolására a Beszállító hálózatáról egy másik célállomásra. Ezt a jogosultságot alapértelmezés szerint meg kell akadályozni.
- g. Citi-adatok feltöltése külső webhelyekre, beleértve a SaaS/fájlmegosztó webhelyeket. Ezt a jogosultságot alapértelmezés szerint meg kell akadályozni.

17.56 Webböngészés

1. A Beszállítónak webhozzáférési szabályozással kell rendelkeznie annak érdekében, hogy a Citi-adatokhoz hozzáféréssel rendelkező munkavállalók esetében elkerülje a Bizalmas vagy magasabb szintű Citi-adatok megosztását, valamint a kártevőknek vagy támadásnak való kitettséget.
2. Azon Beszállítók esetében, akik hozzáféréssel rendelkeznek Bizalmas vagy magasabb besorolású Citi-adatokhoz:
 - a. Minden URL-kérést naplózni kell.
 - b. Le kell tiltani az olyan webhelyek (például webmail, chat, közösségi média, online tárhely, generatív MI stb.) elérésére irányuló kísérleteket, amelyek alkalmasak a Citi-adatok jogosulatlan megosztására.
 - c. Le kell tiltani minden olyan weboldalhoz való hozzáférést, amely kártevőknek vagy támadásnak teheti ki a környezetet.
 - d. A nem üzleti jellegűnek ítélt webhelyekhez való hozzáférési kísérleteket le kell tiltani.
 - e. A Beszállító köteles előfizetést fenntartani egy rendszeresen frissülő URL-kategorizálási szolgáltatásra; minden nem kategorizált URL-t alapértelmezés szerint le kell tiltani, illetve minden URL-t alapértelmezés szerint blokkolni kell, és eseti alapon kell jóváhagyni.
 - f. A Beszállító által használt webböngészőknek teljes mértékben támogatottnak és naprakészeknek kell lenniük a szoftvergyártó legújabb biztonsági frissítéseivel.

17.57 Elektronikus üzenetküldés

Azonnali üzenetküldő eszközök, társközi hálózatok és más kollaboratív internetes eszközök nem használhatók Citi-információk a Beszállító hálózatán kívüli tárolására, a Beszállító hálózatán kívülre történő továbbítására vagy Citi-információkat tartalmazó hálózatokról történő továbbítására, kivéve a 17.9. fejezetben (Kriptográfiai ellenőrzések alkalmazására vonatkozó szabályzat) megadott megfelelő titkosítás alkalmazása esetén.

17.58 E-mail

A Beszállító köteles e-mailekre vonatkozó ellenőrzéseket alkalmazni, hogy megelőzze a Citi-információk megosztását, és mérsékelje a kártevő szoftvereknek és támadásoknak való kitettségét. Ezek közé tartoznak a következők:

1. Az e-mail-átjáróba érkező csatolmányok átvizsgálása és blokkolása, ha azok kockázatot jelentenek a rendszerre nézve.
2. Használatban lévő, naprakész e-mail-szűrés (levélszemétszűrő, adathalászat elleni védelem).
3. Minden Bizalmas vagy magasabb besorolású Citi-adatot titkosítani kell, ha a Beszállító szervezetén kívülre továbbítják.
4. A Beszállító által használt e-mail-klienseknek teljes mértékben támogatottnak kell lenniük és rendelkezniük kell a szoftverforgalmazó által biztosított legújabb biztonsági frissítésekkel.

17.59 Cserélhető adathordozók

1. A beszállító köteles gondoskodni a Citi-információk védelméről, függetlenül attól, hogy azok milyen adathordozón vannak tárolva. Ez a szabály – nem kizárólagosan – a következő, információkat tartalmazó adathordozó-típusokra vonatkozik: kártya, kazetta, CD, lemez vagy más cserélhető adattároló eszköz, nyomtatott példányok, mágneses lemez, mágneses szalag, mikrofilm, mikrolap, optikai lemez vagy papír alapú dokumentum.
2. Azokon a rendszereken, amelyeken Citi-információkat tárolnak, alapbeállításként le kell tiltani a hordozható adattárolókhoz/tárolóeszközökhöz való hozzáférést. Ha kivételek engedélyezésekor megadják az olvasási-írási hozzáférést, akkor az adatokat titkosítani kell a hordozható adattárolón.
3. Cserélhető adathordozók engedélyezett használata esetén az ezen irányú használatot vezető általi jóváhagyási eljáráshoz kell kötni, beleértve a cserélhető adathordozó használatát megkövetelő üzleti szempontot is. A cserélhető adathordozókról a vezetőségnek leltárt kell vezetni. A Bizalmas vagy magasabb szintű Citi-adatokat tartalmazó cserélhető adathordozók titkosításának automatikusan kell megtörténnie, anélkül, hogy szükség lenne a felhasználó beavatkozására.

17.60 Adatok megsemmisítése

1. Amennyiben Bizalmas vagy magasabb besorolású Citi-információk a Citi utasításai szerint megsemmisíthetővé válnak (akkor, amikor a Citinek már nincs szüksége az adott információkra, vagy azok nem hasznosak a számára, valamint lejárt minden törvény, szabályozás és/vagy Citi-irányelv által előírt megőrzési időszak), a Beszállító köteles úgy megsemmisíteni az információkat, hogy azok használhatatlanná és helyreállíthatatlanná váljanak.

2. A csatlakoztatható adathordozók biztonságos törléséhez olyan jóváhagyott eszközt kell használni, amely véletlenszerűen felülírja a meghajtó szektorait meghatározott, eltérő karakterekkel, a következő szabályok alapján:
 - a. A Bizalmas vagy annál magasabb minősítésű információkat tartalmazó adathordozók esetében az alkalmazott törlőeszköznek az adathordozón három egymást követő felülírást kell végrehajtania.
 - b. Az adathordozó lemágnesezése (adott esetben).
3. Az adathordozókat fizikailag meg kell semmisíteni, hogy olvashatatlaná váljanak (azaz aprítást kell végezni, a meghajtókat össze kell zúzni).
4. A Bizalmas vagy magasabb besorolású információkat tartalmazó papíralapú és egyéb nem elektronikus adathordozókat biztonságosan össze kell gyűjteni és egy biztonságos „Bizalmas tárolóban” kell tárolni a végső ártalmatlanításig. A Bizalmas tárolókat mindig zárva kell tartani, csak az arra jogosult személyzet nyithatja ki őket.
 - a. A fénymásolókat, nyomtatókat, faxgépeket és minden más olyan eszközt, amelynek memóriája/tárhelye Bizalmas vagy magasabb besorolású Citi-információkat tartalmazhat, szintén törölni kell.

17.61 Információbiztonsági menedzsment és képzés

1. A Beszállítónak megfelelő kiberbiztonsági és információbiztonsági tudatossági, valamint oktatási programot kell fenntartania, amely többek között kiterjed az adathalász és egyéb pszichológiai manipulációs támadások megelőzésére, a bizalmas vagy annál magasabb minősítésű információk megfelelő kezelésére, valamint a biztonsági incidensek bejelentésére és kezelésére.
2. A Beszállító köteles gondoskodni arról, hogy minden alkalmazott, beleértve az alvállalkozókat és az ideiglenes alkalmazottakat is, tudatosság növelésére irányuló megfelelő oktatásban és képzésben részesüljön a munkaköréhez kapcsolódó szervezeti irányelvek és eljárások tekintetében.
3. A Beszállítónak biztosítani kell, hogy a képzési és tudatosságnövelő programot évente felülvizsgálják és aktualizálják annak érdekében, hogy az figyelembe vegye az újonnan megjelenő kockázatokat és fenyegetéseket, az aktuális bevett gyakorlatokat, valamint a kiberbiztonság területén megjelenő új technológiákat.
4. A képzésnek érintenie kell legalább a következő témákat:
 - b. Információ címkézése és kezelése
 - c. Biztonságos továbbítás (biztonságos e-mail, biztonságos SharePoint-tárhely, a Citi tulajdonában lévő adatok személyes e-mail-címre való küldésének tilalma)
 - d. Információbiztonsági incidens jelentése
 - e. Biztonságos munkakörnyezet (pl. az internet megfelelő használata, jogosulatlan szoftverek használatának tilalma, nem jóváhagyott szoftverek letöltésének tilalma)
 - f. Jelszókezelés (pl. erős jelszavak használata, a jelszavak megosztásának tilalma)
 - g. Pszichológiai manipuláció (adathalászat, személyre szabott adathalászat, telefonos adathalászat és SMS-adathalászat)

- h. Távoli munkavégzés (pl. biztonságos hálózati kapcsolat, biztonságos személyes eszközök)
- 5. A Beszállító alkalmazottainak képzését a Citi-adatokat tároló rendszerekhez való hozzáférés megadásakor vagy azt megelőzően kell elrendelni, és a képzést a megbízásról való értesítésben szereplő határidőig be kell fejezni.
 - a. Amennyiben azt jogszabály nem tiltja, az információbiztonsági képzést valamennyi érintett személy részére legalább évente egyszer meg kell tartani.
- 6. Amennyiben a helyi jogszabályok ezt lehetővé teszik, a képzésnek tartalmaznia kell a hatékonyság mérésére szolgáló dokumentált értékelést (például a képzés végén kitöltendő tesztet, meghatározott megfelelési küszöbértékkel).

17.62 Kiberkockázat-kezelési program

A Beszállítónak emellett legalább egy megfelelő kiberkockázat-kezelési programot kell fenntartania, amelynek legalább az alábbi elemeket kell tartalmaznia:

1. Megfelelően meghatározott és dokumentált Információbiztonsági kockázatkezelési program, és/vagy olyan működési kockázatkezelési program fenntartása, mely rendelkezik a Beszállító kiberkockázat-vállalási hajlandóságát egyértelműen meghatározó kiber-/információs kockázatkezelési komponenssel, és biztosítja, hogy a fennmaradó kiberkockázat igazodjon ahhoz a hajlandósághoz.
2. Hatékony biztonsági kockázatkezelési program fenntartása, mely többek között magában foglalja a szervezeten belüli általános biztonsági állapot kiértékelésére szolgáló biztonsági auditok és felülvizsgálatok összegyűjtését és/vagy elvégzését, és mely legalább évente jelentést készít a szervezet vezetősége számára felülvizsgálati célból, valamint annak biztosítására, hogy nem sérült a Beszállító kiberkockázat-vállalási hajlandósága.
3. A Beszállítóra vonatkozó PCI adatbiztonsági szabványoknak (PCI-DSS) való megfelelés fenntartása, ha a Beszállító hitelkártyákkal/betéti kártyákkal folytatott tranzakciókat, kifizetéseket és/vagy kapcsolódó információkat dolgoz fel, tárol és/vagy továbbít.
4. Olyan válságkezelési terv és forgatókönyv, valamint Biztonsági eseményekre reagáló csoportra vonatkozó terv fenntartása, amely megfelel az iparági szabványoknak, és biztosítja, hogy a Beszállító elegendő és megfelelő képességekkel rendelkezik a megkísérelt, vélelmezett és/vagy tényleges kiberbiztonsági incidensek észlelésére, megfékezésére, kivizsgálására, valamint az azokra való reagálásra és a helyreállításra.

17.63 Alkalmazás-, API-, kód-, rendszer- és infrastruktúra-biztonság

Amennyiben a Beszállító szoftveralkalmazást/szoftveralkalmazásokat üzemeltet, fejleszt, társfejlesztésben vesz részt, fejlesztői környezetet biztosít és/vagy szállít, köteles elvégezni az adott szoftverek és/vagy a szoftverhez tartozó javítások kódjának vizsgálatát biztonsági hibák, jogosulatlan hozzáférés, rosszindulatú programok és más rosszindulatú kód, módosítás beillesztésének megakadályozása, valamint sebezhetőségi tesztelés céljából. Ezáltal biztosítani kell, hogy az alkalmazás (beleértve az API-kat is), az alapul szolgáló rendszerszolgáltatásokkal, operációs rendszerekkel és hálózatokkal együtt, mentes legyen az ismert sebezhetőségektől és hibáktól, melyek

biztonsági vagy adatvédelmi incidenst, csalást, jogosulatlan hozzáférést és/vagy Bizalmas információk megosztását, az alkalmazás(ok) által feldolgozott, tárolt vagy továbbított információk integritásának elvesztését és/vagy a rendelkezésre állás elvesztését eredményezhetik, és ezáltal befolyásolhatják a Beszállító által a Citinek nyújtott termékek és/vagy szolgáltatások minőségét.

17.64 Mobilbiztonság

Ha a Beszállító mobilalkalmazás-megoldást szolgáltat, akkor meg kell felelnie a következő követelményeknek:

1. A mobilalkalmazás kizárólag a Google Android (az Android Go kivételével), illetve az Apple iOS/iPadOS általánosan elérhető (GA), stabil és még támogatott (nem EOL²) verzióit támogathatja. Amennyiben a mobilmegoldás további operációs rendszereket vagy verziókat is támogat, azok körének a Citi által konfigurálhatónak kell lennie.
2. A mobilmegoldás nem támogathat olyan mobilplatformokat/-eszközöket, melyek nincsenek felszerelve a kriptográfiai algoritmusokat támogató bevett utasításkészletekkel, beleértve többek között a jelen dokumentum 17.9. (Titkosítási követelmények) fejezetében meghatározott titkosítást.
3. Az operációs rendszer kereskedelmi forgalom előtti verzióinak éles környezetben való használata nem engedélyezett, beleértve, a teljesség igénye nélkül, a béta, korai hozzáférésű és funkcióelőnézeti verziókat/kiadásokat is.
4. A Beszállítónak képesnek kell lennie arra, hogy megadja a harmadik féltől származó integrált komponensek listáját, beleértve többek között, de nem kizárólagosan a mobilmegoldás által csomagolt/felhasznált ingyenes és nyílt forráskódú szoftverkönyvtárakat.
5. A mobilalkalmazásnak meg kell felelnie azoknak a követelményeknek és bevált gyakorlatoknak, melyek lehetővé teszik a mobilalkalmazások közzétételét nyilvános alkalmazás-áruházakban, például az Apple App Store és a Google Play Store áruházakban. A felsorolt nyilvános alkalmazás-áruházak jelentik a preferált és elsődleges módszert a mobilalkalmazás terjesztésére/közzétételére.
6. Az Android-mobilalkalmazásoknak az APK aláírási séma 2-es vagy újabb verzióját kell használniuk. Az APK aláírási séma 1-es verziója (más néven JAR-aláírás) nem használható.
7. A mobilalkalmazás aláírási kulcsának típusának és hosszának meg kell felelnie a jelen dokumentum 17.9. – Titkosítási **követelmények** című fejezetében foglaltaknak.
8. Minden alkalmazás aláírási kulcsot és kapcsolódó X.509v3 tanúsítványt külön kell kezelni, és egyetlen alkalmazásazonosítóhoz/csomagazonosítóhoz kell rendelni. Az aláírási kulcs(ka)t tilos megosztani az alkalmazások között.

² Olyan termékverziók, amelyek aktívan támogatottak, és rendszeres biztonsági és karbantartási frissítéseket kapnak a platform tulajdonosától vagy a Beszállítótól.

9. Ha egy mobilalkalmazáshoz adatok mobileszközön való tárolása szükséges, akkor kizárólag azokat a legfrissebb adatokat lehet tárolni az eszközön, amelyek az alkalmazás/szolgáltatás céljához/céljaihoz szükségesek, illetve addig lehet tárolni őket, ameddig azt jogszabályi vagy szabályozási követelmények előírják.
 - a. A felhasználói adatok gyűjtésének, feldolgozásának és/vagy tárolásának meg kell felelnie a helyi törvényeknek, beleértve többek között, de nem kizárólagosan az adatvédelmi előírásokat, például az általános adatvédelmi rendeletet (GDPR) és a 2002/58/EK (e-adatvédelmi) irányelvet vagy azok helyi megfelelőit.
 - b. A harmadik féltől származó integrált komponensek (pl. könyvtárak) nem gyűjthetnek, dolgozhatnak fel és/vagy tárolhatnak felhasználói adatokat.
10. A mobilalkalmazások semmilyen alkalmazásadatot sem tehetnek nyilvánosan elérhetővé.
 - a. Ha adatok más alkalmazásokkal való megosztására van szükség, akkor az alkalmazásoknak az adott operációs rendszerekre vonatkozó, kereskedelmi szempontból észszerű technikákat, módszereket és ellenőrzéseket kell alkalmazniuk, hogy kizárólag a szükséges mennyiségű adatot osszák meg, a lehető legkevesebb egyéb alkalmazással, azzal a feltétellel, hogy az adatmegosztásnak megfelelően indokoltnak és dokumentáltnak kell lennie.
11. A mobilalkalmazások kizárólag az adott mobil operációs rendszerek által biztosított biztonságos kommunikációs lehetőségekre támaszkodhatnak. Például:
 - a. Az Android-alkalmazásoknak kifejezetten nyilatkozniuk kell az alkalmazásjegyzékben és/vagy a hálózati konfigurációs fájlban arról, hogy a nem biztonságos hálózati forgalom egyetlen hálózati tartomány felé sem engedélyezett.
 - b. Az iOS/iPadOS alkalmazásoknak kivétel nélkül használniuk kell az alkalmazások átviteli biztonsága (Application Transport Security/ATS) funkciót.
12. A kriptográfiai anyagokat hardverrel támogatott biztonságos kulcstárhoz kell kötni.
13. A mobilalkalmazásokat kiadási módban kell építeni, és nem tartalmazhatják a következőket:
 - a. Bármilyen olyan funkció vagy módszer, amely megkerülheti a biztonsági ellenőrzéseket,
 - b. Hibakeresési információk, például forráskód részét képező fájlnevek, változónevek, szimbólumnevek stb., amelyek elősegíthetik a visszafejtést.
14. A mobilalkalmazásokat hatékony hooking- vagy manipulációgátló mechanizmusokkal kell ellátni, hogy megakadályozzák olyan rosszindulatú

kódok beillesztését, amelyek futás közben megváltoztathatják vagy figyelhetik az alkalmazás viselkedését.

15. A mobilalkalmazásoknak átfogó technikákat kell alkalmazniuk a hibakeresés vagy a visszafejtés/zavarás gátlására a visszafejtési támadások megakadályozása érdekében.
16. A mobilalkalmazás-csomagoknak lehetővé kell tenniük a tartalom hitelességének és integritásának ellenőrzését (pl. kriptográfiai ellenőrző összeg és/vagy digitális aláírás használatával).
17. Ha a mobilalkalmazás felhasználói hitelesítést igényel, akkor az alkalmazás és/vagy az eszköz integritásának ellenőrzését a felhasználói hitelesítés megkezdése előtt el kell végezni.
18. Azok a mobilalkalmazások, melyek hozzáférnek/feldolgoznak/tárolnak a Citi tulajdonában álló, Bizalmas vagy magasabb Citi-besorolású információkat, és/vagy melyek információbiztonsági besorolása Közepes vagy magasabb, csak erős biometrikus módszereket használhatnak (pl. megfelelnek a megfelelő [Android Compatibility Definition Document](#) meghatározottak szerinti 3. osztálynak/erős kategóriának vagy meghaladják azt).
19. A mobilalkalmazásoknak ellenintézkedés(ek)e)t kell végrehajtaniuk a közbeékelődéses (MitM) támadások elleni védelem érdekében.
20. A mobilalkalmazásoknak képesnek kell lenniük felismerni a feltört eszközöket, beleértve többek között, de nem kizárólagosan a „függetlenített” és a „rootolt” mobilkészülékeket, és a vállalat kockázatértékelési követelményeivel, valamint a szabályozási követelményekkel összhangban kell reagálniuk rájuk.
21. A mobilalkalmazásoknak erős eszközpárosítást kell megvalósítaniuk a szoftvertoken (pl. birtoklási igazolás) klónozásának megakadályozására.
22. A mobilalkalmazásoknak biztonságos billentyűzet-alkalmazásokat/-megoldásokat kell használniuk (pl. azokat, amelyek be vannak építve vagy előre telepítve vannak a mobil operációs rendszerekre).
23. A leküldetéses értesítések nem tartalmazhatnak érzékeny információkat (pl. Bizalmas vagy magasabb besorolású Citi-információkat). Az egyszeri jelszó azonban leküldetéses értesítésen keresztül is kiosztásra kerülhet.
24. A mobilalkalmazás-megoldásoknak képesnek kell lenniük az olyan mobilkliensekkel való kommunikációs kísérletek elutasítására/figyelmen kívül hagyására, amelyek ismert/kihasználható sebezhetőséggel rendelkező alkalmazásverzió(ka)t használnak.
25. A mobilalkalmazásoknak meg kell felelniük az iparág bevált gyakorlatainak, beleértve a következő oldalon közzétett megelőzési technikákat is: [OWASP Mobil Top 10](#).
26. Ha a mobilalkalmazás mesterséges intelligenciát és gépi tanulási (AI/ML) technikákat hasznosít, akkor azt etikus módon, valamint a 19. – Mesterséges intelligencia/gépi tanulás (beleértve a generatív mesterséges intelligenciát és az autonóm ügynök alapú mesterséges intelligenciát is) című fejezetnek megfelelően kell tennie.

27. A mobilalkalmazásnak az(oka)t a minimális eszközendély(eke)t kell használnia, amely(ek) szükséges(ek) a Citi által használt cél(ok)/funkció(k) végrehajtásához.
28. A mobilalkalmazások semmilyen nem nyilvános információt nem tárolhatnak külső/cserélhető tárolóeszközökön, például SD-kártyákon.**Error! Reference source not found.**

17.65 Szoftverkomponensek nyilvánosságra hozatala

A Beszállítónak nyilvánosságra kell hoznia a Citi részére nyújtott termékekben vagy szolgáltatásokban található valamennyi szoftverkomponenst – beleértve többek között a nyílt forráskódú szoftvereket is (együttesen „Szoftverkomponensek”). A Beszállító nem építhet be frissítés, verzióváltás útján vagy más módon új Szoftverkomponenst a Citi rendszereire telepítendő termékek vagy szolgáltatások egyetlen verziójába sem anélkül, hogy erről előzetesen tájékoztatta volna a Citit. A Beszállítónak továbbá biztosítania kell, hogy termékei vagy szolgáltatásai ne tartalmazzanak olyan Szoftverkomponenseket, amelyek licence a Citire vagy kapcsolt vállalkozásaira a Citi által valamely szerződésben kifejezetten el nem ismert és el nem fogadott kötelezettségeket róna. A Beszállítónak az észleléstől számított 30 napon belül tájékoztatnia kell a Citit a szervezetében, termékeiben vagy szolgáltatásaiban azonosított valamennyi rosszindulatú Szoftverkomponensről. A Beszállítónak a termékek vagy szolgáltatások minden egyes kiadásához és verziójához kapcsolódóan Szoftverjegyzéket („SBOM”) kell a Citi rendelkezésére bocsátania, OWASP CycloneDX vagy ISO/IEC 5962:2021 Software Package Data Exchange („SPDX”) fájlformátumban, amely tartalmazza a felhasznált Szoftverkomponenseket. A közölt információknak tartalmazniuk kell a Szoftverkomponensek eredetét (például kereskedelmi szállító, beágyazott adatbázis, nyilvános bináris csomagkezelő, forráskódból fordított komponens, beágyazott szoftver vagy válogatott szoftverkomponens-szolgáltató), továbbá azt is, hogy a Beszállító, illetve a szoftverellátási lánc bármely résztvevője készítette-e a komponensről másolatot („fork”), amelyet ezt követően csomagfüggőségként vagy a Beszállító forráskódjába integrált forráskódként épített be a termékbe vagy szolgáltatásba.

17.66 Fenyégetésmodellezés

A Beszállítónak olyan fenyegetésmodellezési folyamatot kell bevezetnie, amely átfogó módon lefedi, illetve magában foglalja legalább az alábbiakat:

1. A hatókör meghatározása: A Beszállítónak egyértelműen meg kell határoznia a fenyegetésmodell hatókörét, különös tekintettel azokra a szoftverkomponensekre és adatfolyamokra, amelyek Bizalmas vagy annál magasabb minősítésű Citi-információkat dolgoznak fel, tárolnak vagy továbbítanak.
2. Fenyégetések azonosítása: A Beszállítónak szisztematikus módon azonosítania kell a szoftver tervezésével, architektúrájával és rendeltetésszerű használatával összefüggő lehetséges fenyegetéseket és sérülékenységeket, már a tervezési életciklus korai szakaszában figyelembe véve a különböző támadási módszereket és fenyegető szereplőket.

3. Kockázatelemzés: A Beszállítónak elemeznie kell az azonosított fenyegetéseket azok várható hatásának és bekövetkezési valószínűségének felmérése érdekében, lehetővé téve a biztonsági kockázatok rangsorolását.
4. Ellenőrzés integrálása: A Beszállítónak a rangsorolt kockázatok kezelésének érdekében meg kell határoznia és a szoftver tervezési és fejlesztési folyamatába be kell építenie a megfelelő biztonsági ellenőrzéseket és kockázatcsökkentő megoldásokat.
5. Dokumentáció: A Beszállítónak dokumentálnia kell a fenyegetésmodellt, beleértve az azonosított fenyegetéseket, a kapcsolódó kockázatokat és a végrehajtott kockázatcsökkentő intézkedéseket.
6. Időszakos felülvizsgálat: A Beszállítónak rendszeresen felül kell vizsgálnia és szükség szerint frissítenie kell a fenyegetésmodelleket, különösen akkor, ha a szoftver kialakításában, funkcionalitásában vagy telepítési környezetében jelentős változás történik.

17.67 Mesterséges intelligencia

1. A Beszállítónak a Citi részére biztosított vagy a Citi rendszereibe integrált valamennyi mesterséges intelligencia/gépi tanulási (MI/ML) rendszerre és komponensre vonatkozóan biztonságos szoftverfejlesztési életciklust (SSDLC) kell kialakítaniuk és alkalmazniuk. Ez magában foglalja a biztonságos tervezést, fejlesztést, tesztelést, üzembe helyezést és a folyamatos karbantartást.
2. A Beszállító által biztosított MI-rendszereknek működésük során biztosítaniuk kell a kellő integritást, valamint magas szintű ellenálló képességet kell tanúsítaniuk a támadásokkal szemben. Ennek részeként meg kell valósítani az utasítás injekciók felismerését, a bemeneti adatok ellenőrzését és tisztítását, valamint az adatok elkülönítését biztosító mechanizmusokat.
3. A Beszállító által biztosított MI-ügynökök és egyéb MI-komponensek kizárólag biztonságos módon kommunikálhatnak a Citi rendszereivel és egyéb eszközeivel. Ennek érdekében erős identitás- és hozzáférés-kezelést kell alkalmazni, szigorúan ellenőrizni kell az eszközök futtatási paramétereit, valamint el kell különíteni a magas kockázatú műveleteket végző eszközöket. Az érzékeny vagy magas kockázatú műveletek esetében emberi felügyeleti mechanizmusokat (HITL) kell alkalmazni.
4. A Beszállító MI-rendszereinek minden jelentős eseményről teljes körű, megváltoztathatatlan és auditálható naplókat kell generálniuk. Ezeket a naplókat védeni kell a jogosulatlan módosítás ellen, központilag össze kell gyűjteni, és a Citi előírásainak megfelelően kell megőrizni. Folyamatos monitorozási és anomáliaészlelési képességeket kell biztosítani a biztonsági szempontból releváns események és a gyanús tevékenységek felismerésére, valamint az ezekkel kapcsolatos riasztások kiadására.
5. A Beszállító MI-rendszereinek támogatniuk kell a kockázatalapú emberi felügyeletet, lehetővé téve a megfelelő beavatkozást, és a felelősség egyértelmű megállapítását az MI-eredmények és -műveletekért tekintetében. Ennek része az MI-eredmények kockázati szint szerinti besorolása, valamint az emberi felülbírálat lehetőségének biztosítása.
6. A Beszállító által biztosított valamennyi MI-ügynöknek, MI-komponensnek és MI-rendszernek erős identitás- és hozzáférés-kezelési kontrollokat kell alkalmaznia. Minden MI-vel folytatott interakciónak egyértelműen

hozzárendelhetőnek kell lennie egy azonosítható (emberi vagy nem emberi) identitáshoz, és minden hozzáférés esetében hitelesítést kell alkalmazni. Az MI-ügynököknek kezelt identitásokat kell használniuk, és a Citi erőforrásaihoz való hozzáférés során a legkisebb jogosultság elvét kell alkalmazniuk.

- a. A Beszállítóknak biztosítaniuk kell, hogy valamennyi MI-ügynök Citi Object Identity Network (COIN) ügynökazonosítót kapjon, amely össze van kapcsolva a Citi Identity and Access Management (IAM) rendszereivel, így biztosítva a Citi biztonsági szabályzatainak érvényesítését, a központi identitáskezelést és az auditálhatóságot.
 - b. A Beszállítóknak a harmadik fél által biztosított ügynököket a Citi által jóváhagyott integrációs mechanizmusok alkalmazásával kell a COIN rendszerhez csatlakoztatniuk, beleértve a biztonságos átjárókon (például SSG Gateway vagy Apigee) keresztül elérhető COIN API használatát is. Biztosítaniuk kell továbbá, hogy a csatlakoztatás a Citi vonatkozó biztonsági követelményeinek megfelelően, biztonságos módon történjen.
 - c. Ha a Beszállító megoldása belső üzemeltetésű, akkor a COIN rendszerrel kompatibilis token-t kell generálni. Külső üzemeltetés esetén, amennyiben a hitelesítés saját federált token-nel történik, biztosítani kell a Citi tokenjeivel kompatibilis támogatott tokenátalakítást (például MSFT tokenről COIN tokenre történő átváltást). Minden olyan új tokentípust, amelyet az átváltási mechanizmus jelenleg nem támogat, a Citi IAM csapatának jóvá kell hagynia.
7. Amennyiben a Beszállító Model Context Protocol (MCP) szervereket vagy klienseket használ vagy biztosít, az MCP RFC 7591 szabványt kell implementálnia – annak valamennyi opcionális funkciójával együtt.
 8. A Beszállító MI-rendszereinek védeniük kell a rendszerutasításokat és a belső működést a jogosulatlan hozzáféréssel, nyilvánosságra hozatallal és manipulációval szemben. A kontextuskezelésnek szigorú elkülönítést kell biztosítania, hogy megakadályozza az adatszivárgást a különböző ügyfelek, felhasználók vagy környezetek között.
 9. A Beszállítóknak dokumentált eljárásokkal kell rendelkezniük az MI-hez kapcsolódó biztonsági incidensek felismerésére, kezelésére és bejelentésére, beleértve a támadásokat, a modellek manipulálását, a jogosulatlan MI-műveleteket, valamint az MI-rendszereket érintő adatvédelmi incidenseket is. A Citit azonnal értesíteni kell minden ilyen incidensről.

18 MUNKAHELYI BIZTONSÁGGAL KAPCSOLATOS IRÁNYMUTATÁSOK

Azokra a Beszállítókra vonatkozik, akik Citi-információkat elérnek/feldolgozzák/kezelik/tárolják ÉS/VAGY Citi márkájú, internetre optimalizált alkalmazásokat üzemeltetnek ÉS/VAGY kapcsolattal rendelkeznek a Citi hálózati erőforrásaihoz ÉS/VAGY kíséret nélküli hozzáférést igényelnek a Citi létesítményeihez.

A Beszállítók kötelesek gondoskodni a Citihez és a Citi Ügyfeleihez tartozó tárgyi eszközök és immateriális javak biztonságáról. A Citi és az Ügyfél eszközei csak jóváhagyott célokra és jóváhagyott módon használhatók fel (pl. a vonatkozó engedélyeknek, feltételeknek megfelelően), és akkor is csak a Citi és a Citi Beszállítóinak üzleti céljaira tekintettel. Az eszközök közé tartoznak a következők: készpénz, értékpapírok, vagyontárgyak, szolgáltatások, üzleti tervek, Citi-információk, Beszállító információi, forgalmazói információk, szellemi tulajdon (számítógépes programok, modellek és egyéb tételek), valamint minden egyéb személyes, védett és Bizalmas információ. A Citi eszközeinek jogosulatlan eltulajdonítása vagy jogosulatlan felfedése az Ön Citivel szembeni kötelezettségének megszegését jelenti, és a Citivel szemben elkövetett csalásnak minősülhet. Hasonlóképpen a Citi eszközeivel kapcsolatban elkövetett gondatlanság, pazarlás vagy jogosulatlan használat szintén kötelezettségszegésnek minősül.

Tétel	Követelmények
Citi információk (elektronikus és nyomtatott dokumentumok)	Zárja el és biztosítsa a Citi információkat a szokásos munkaidőt követően, illetve bármikor, amikor a Beszállító távol van a kijelölt munkaterülettől.
Asztali személyi számítógépek (PC-k) és laptopok	A Citi információk elérésére vagy megtekintésére használt számítógépeket és laptopokat egy adott inaktív időszak elteltét követően képernyővédő jelszavakkal kell levédeni. Amikor a Beszállító elhagyja a kijelölt munkaterületet, le kell zárnia a számítógépet és/vagy laptopot a CTRL + ALT + DEL billentyűkombináció, majd pedig a „Számítógép zárolása” lehetőség kiválasztásával. Ha a Beszállító laptopot használ a Citi információk megtekintéséhez, a Beszállítónak gondoskodnia kell arról, hogy az ilyen laptopot munkaidő alatt kábellel vagy biztonsági zárral rögzítse a dokkoló állomáshoz, a szokásos munkaidő után pedig biztonságosan elzárja.
Zárja el	A Citi-információkat tároló irattartó szekrényeket és fiókokat a szokásos munkaidő végén zárni kell.
Nyitott iroda	A nyitott irodaterületeket tilos fájlserverként/mini-adatközpontként használni Citi-információk tárolására, kivéve, ha azokat kifejezetten ilyen célra tervezték, és használatukat a Citivel dokumentálták.
Nyomtatók, fénymásolók és faxgépek tálcái	Minden Citivel kapcsolatos anyagot el kell távolítani a nyomtatókról, fénymásolókról és faxgépekről.
Megsemmisítés	Semmisítse meg a már nem szükséges Citi-információkat (kövesse a meghatározott megőrzési ütemterveket). A dokumentumokat aprítógépbe kell dobni, vagy egy biztonságos/zárt szemeteskosárba kell helyezni. A mágneses adathordozókat biztonságosan kell megsemmisíteni, miután elvégezte a megfelelő törlési eljárásokat.

19 MESTERSÉGES INTELLIGENCIA/GÉPI TANULÁS (BELEÉRTVE A GENERATÍV MESTERSÉGES INTELLIGENCIÁT ÉS AZ AUTONÓM ÜGYNÖK ALAPÚ MESTERSÉGES INTELLIGENCIÁT IS)

E követelmények azon Beszállítókra alkalmazandók, amelyek a Citi által a jelen Beszállítói követelményekben meghatározott mesterséges intelligenciát/gépi tanulást (MI/ML) – beleértve a generatív és agentikus mesterséges intelligenciát is – az általuk nyújtott termék vagy szolgáltatás bármely részében alkalmazzák.

19.1 A Beszállító nem alkalmazhatja – és köteles biztosítani, hogy alvállalkozói se alkalmazzák – az alábbiakban meghatározott MI/ML-technológiákat, kivéve, ha azok használatában a Felek a Szerződés vonatkozó mellékletében vagy munkamegrendelésében kifejezetten megállapodtak:

- a. Olyan termék vagy szolgáltatás felhasználásában, tartalmaként vagy részeként, amelyre vonatkozóan Szerződést kötnek, hogy közvetlenül vagy közvetve biztosítsák a Citi, vagy annak bármely része számára, beleértve az abban foglalt vagy abba beágyazott, harmadik féltől származó termékeket vagy szolgáltatásokat; vagy
2. A Beszállító bármely Szerződésének teljesítése során felhasználva, függetlenül attól, hogy az ilyen MI-t/ML-t a Citinek biztosított tényleges termék vagy szolgáltatás felhasználja, tartalmazza, illetve annak részét képezi-e; vagy
3. A Beszállító által oly módon felhasználva, hogy az Citi-információkat tehet ki ezen MI-nek/ML-nek, ideértve a Beszállító által nem kereskedelmi tevékenységei során felhasznált MI-t/ML-t is (pl. üzleti nyilvántartások vezetése, folyamatfejlesztések, kutatás és fejlesztés, megfelelés és belső ellenőrzés).

19.2 Ha a Beszállító nem tesz eleget ezen kötelezettségeinek, az a jelen Szerződésben foglalt feltételek lényeges megszegésének minősül.

19.3 Ha a szabályozó kéri, az MI-t/ML-t egy termék/szolgáltatás bármely részében történő felhasználásával kapcsolatos hatósági ellenőrzés vagy törvényszéki vizsgálat részeként a Beszállítónak segítenie kell a Citit a szabályozó kérésének megválaszolásában, beleértve az MI-t/ML-t alkotó algoritmusok tényleges működésének felderítéséhez szükséges algoritmus ellenőrzésének elvégzését és/vagy ilyen ellenőrzés elvégzését.

19.4 A következő elveket is be kell tartani:

Jogszerűség. A Beszállító által használt Mesterséges intelligenciának/Gépi tanulásnak meg kell felelnie az Alkalmazandó jogszabályoknak.

Cél és arányosság. A Beszállító nem egyesítheti a Tartalmat vagy a Citi-információkat a Beszállító vagy harmadik fél adataival. A Beszállító a Citi írásbeli jóváhagyása nélkül nem használhatja fel a Tartalmat vagy a Citi-információt Mesterséges intelligencia/Gépi tanulás betanítására. A Beszállító által alkalmazott Mesterséges intelligencia/Gépi tanulás csak a Szolgáltatások nyújtásához szükséges mértékben használhat fel Tartalmat vagy Citi-információt.

20 ÜGYFÉLPANASZOK

20.1 A Panasz egy szóbeli vagy írásbeli közlés, melyet benyújthatnak szóban (személyesen vagy telefonon) vagy írásban (postai úton vagy elektronikus kommunikációs eszközökön, például e-mailben, chaten vagy közösségi médiában stb.), és melyben egy Ügyfél, nem Ügyfél, leendő Ügyfél, Citi-ügyfél, vagy egy Ügyfél meghatalmazott képviselője (együttesen: „Ügyfél”) elégedetlenséget fejez ki egy Citi-szabályzattal, -termékkel vagy -szolgáltatással kapcsolatban, melyet a Citi, egy Citi-alkalmazott, Citi-alvállalkozó vagy a Citi nevében eljáró harmadik fél vagy ezek bármely kombinációja kínál.

20.2 A Beszállítók kötelesek követni a Citi Ügyfélpanaszok kezelésére vonatkozó szabályzatát, valamint az alkalmazandó Citi Panaszkezelési szabványokat és eljárásokat. A Beszállító köteles a Citi elsődleges üzleti kapcsolattartóját (vagy az általa kijelölt személyt) 24 órán belül írásban értesíteni minden olyan írásbeli vagy szóbeli panaszról vagy kifogásról (külön-külön „Panasz”), amelyet bármely ügyféltől (vagy a Citi panaszfogalma szerinti nem ügyféltől vagy leendő ügyféltől), illetve bármely felügyeleti hatóságtól kap a Citi nevében nyújtott szolgáltatásokkal vagy egyébként a Citivel kapcsolatban. Amennyiben a Citi nem biztosít a Beszállítónak ilyen rendszert, úgy a Beszállító köteles egy a Citi észszerű elvárásainak megfelelő rendszert („Követőrendszer”) is kifejleszteni, bevezetni és fenntartani a Panaszok nyomon követésére, és a Citi számára, a Citi saját belátása szerint meghatározott igénye alapján a jelentésekről másolatot vagy a rendszerhez hozzáférést biztosítani. A Követőrendszernek képesnek kell lennie a következőkre:

- a. a Panaszokat típus, beérkezés dátuma és a Panaszról a Citinek küldött értesítés dátuma szerint kategorizálni,
- b. nyomon követni a Panasz kezelésének menetét a lezárásig/megoldásig, és
- c. gondoskodni minden egyéb olyan üggyről, melyet a Citi észszerűen kérhet. A Követőrendszert úgy kell kialakítani, hogy a Beszállító meg tudja állapítani, ha egy adott üggyel kapcsolatban aránytalanul sok Panasz érkezik hozzá. A Beszállító ezáltal (a Citivel konzultálva) megállapíthatja, hogy van-e a Beszállító üzleti tevékenységével vagy a Szolgáltatások nyújtásával kapcsolatos rendszerszintű probléma, és ezt haladéktalanul orvosolhatja.

21 SZEMÉLYES KERESKEDELMI ÉS BEFEKTETÉSI SZABÁLYZAT

A Citi Személyes kereskedelmi és befektetési szabályzata (PTIP) meghatározza az engedélyezett és tiltott kereskedési és befektetési tevékenységeket, az előzetes engedélyezési követelményeket, valamint az Érintett személyek bróker- és kereskedési számláinak vezetésére, közzétételére és felügyeletére vonatkozó követelményeket. Minimumkövetelményeket határoz meg a törvények és rendeletek betartásának előmozdítása érdekében, hogy megakadályozza a Citinél való munkakörök és a Citivel való kapcsolat nem megfelelő kihasználását, beleértve a következőkkel kapcsolatos egyéni ismeretek felhasználását is: (1) a Citivel vagy egy harmadik féllel kapcsolatos Lényeges nem nyilvános információk vagy bennfentes információk (együttesen „MNPI”); vagy (2) az ügyfelek értékpapírjaira, származtatott és árupiaci pozícióira, tranzakcióira és stratégiáira vonatkozó információk.

A Beszállító minden olyan személyzeti tagja, akinek a Citinél betöltött munkaköri feladatai részeként rendszeres hozzáférésre van szüksége MNPI-hez, és aki Érintett személynek és/vagy Citi-hozzáféréssel rendelkező személynek minősül, köteles betartani a PTIP-ben foglalt követelményeket. A Beszállító munkatársainak eleget kell tenniük az ICRM által a személyes számlák bejelentésére, a személyes kereskedési tevékenységek előzetes engedélyeztetésére, a személyes kereskedelemre vonatkozó korlátozások betartására és az időszakos kimutatások benyújtására vonatkozó előírásoknak.

22 SZÁMLÁZÁS ÉS SZÁMLÁZÁSI SZABVÁNYOK

A Citi a szolgáltatás időszerűségének javítására és az ellenőrzések fokozására irányuló erőfeszítéseivel összhangban minden Beszállító a Citi által előnyben részesített számlabenyújtási módszereket, illetve számlafizetési lehetőségeket köteles használni, az alábbi részletes követelmények szerint:

- A Beszállítónak elektronikus fájlokat kell létrehoznia, melyeket a Citinek továbbít a Citi által a Beszállítóval közölt formátumban, és/vagy a Citi iSupplier eszközének segítségével kell rögzítenie a szükséges számlázási adatokat a Citinek való későbbi digitális továbbításhoz.
- A Beszállító köteles a Citi rendelkezésére bocsátani az összes szükséges banki információt és az igazoló dokumentációt a Beszállítónak történő elektronikus fizetés megkönnyítése érdekében, és/vagy igénybe venni a Citi virtuális kártyás fizetési lehetőségét (ahol elérhető).

Megjegyzés: A fizetési feltételek meghatározása a számla Citi általi kézhezvételének napján alapul.

Az időben történő fizetés és a szerződéses kötelezettségek teljesítése érdekében a Citi minden Beszállító számára előírja, hogy feltüntessék a következő számlaadatokat, és

betartsák a kapcsolódó irányelveket az áruk vagy szolgáltatások Citi felé történő számlázása során:

1. A megfelelő Citi üzleti szervezet, a „Számlázási cím” és a hozzá tartozó Citi üzleti kapcsolattartó neve.
2. Számlaszám, Dátum és a Megrendelés száma.
3. A számlákat a Citi-megrendelésén feltüntetett Citi-fiókba vagy e-mail-címre kell küldeni.
4. A számlán fel kell tüntetni az áruk vagy szolgáltatások világos és részletes leírását.
5. Csak az adott számla aktuális költségeit kell feltüntetni (ne tüntessenek fel egyéb függőben lévő, kifizetetlen számlaegyenleget).
6. A számlákat az igazoló dokumentációval együtt angol nyelven kell kiállítani.

23 KÖTELEZŐ TÁVOLLÉTI IRÁNYELV

A Citi Kötelező Távolléti Irányelve előírja, hogy az érzékeny vagy magas kockázatú – különösen akik a vállalat könyvelését és nyilvántartásait érintő – tevékenységeket végző személyeknek meghatározott időközönként átmenetileg fel kell függeszteniük e feladataik ellátását. A kötelező elkülönítés célja a belső kontrollok megerősítése azáltal, hogy lehetőséget teremt az esetlegesen rejtve maradó csalások, lopások vagy egyéb visszaélések feltárására. Az irányelv összhangban áll az Amerikai FED kormányzótanácsa által az érzékeny munkakörökben dolgozó személyek kötelező távollétére meghatározott felügyeleti elvárásaival.

A Kötelező Távolléti Irányelv előírásait minden olyan Beszállítói munkatártnak be kell tartania, aki a Citinél végzett munkája során érzékeny adatokhoz fér hozzá, és „Érzékeny” személyként van besorolva. Az Érzékeny besorolású személyeknek évente be kell ütemezniük és teljes egészében ki kell tölteniük a Kötelező Távolléti Időszakot a szabályzat valamennyi előírásának és korlátozásának megfelelően. A kötelező távolléti időszak alatt nem végezhetnek, nem irányíthatnak, nem engedélyezhetnek és nem hagyhatnak jóvá érzékeny tevékenységeket, továbbá érdemben nem válaszolhatnak semmilyen megkeresésre – beleértve az ügyfelekkel folytatott kommunikációt is –, kivéve, ha kizárólag a kijelölt helyetteshez irányítják az érdeklődőt. Amennyiben a kötelező távolléti időszak megkezdését követően azt meg kell szakítani, a vezetőnek vagy a Citi üzleti kapcsolattartójának a Megfelelőségi rendszerekben meg kell szakítania azt a rendszerhozzáférések visszaállítása érdekében. Ezt követően az érintett munkavállalónak új kötelező távolléti időszakot kell ütemeznie.

FÜGGELÉK – FOGALOMMEGHATÁROZÁSOK

Légrés: biztonsági intézkedés, melynek keretében egy számítógépet, rendszert vagy hálózatot fizikailag elválasztanak más számítógépektől, rendszerektől vagy hálózatoktól. Egy légrés megoldást alkalmazó biztonsági mentéses architektúra korlátozza a kibertámadásoknak való kitettséget, és lehetővé teszi az adatok visszaállítását a támadás kezdete előtti időpontra.

Az **Alkalmazandó jogszabályok** magukba foglalják a következőket: a) állami felszámolási törvények és rendeletek, valamint b) az Egyesült Államok különböző szövetségi ügynökségei, köztük a Pénzügyi Ellenőrzési Hivatal által kibocsátott szabályok, iránymutatások és egyéb közlemények, amelyek a 2003-ban elfogadott, a tisztességes és pontos hitelügyletekről szóló törvény 114. szakaszát hajtják végre („piros zászlós iránymutatások és rendelkezések” [Red Flag Guidelines and Regulations] néven is ismeretesek)

Rendelkezésre állási zóna: az a hely, ahol a felhőszolgáltató logikai adatközpontok csoportjával rendelkezik. A Rendelkezésre állási zóna magába foglal egy vagy több különálló adatközpontot redundáns energiaellátással, hálózattal és telekommunikációval egy adott Felhőrégióban.

A **Mesterséges intelligencia (MI)** olyan kvantitatív módszert, rendszert vagy megközelítést („technikát”) jelent, amely számítógépes programok segítségével utánozza az emberi intelligenciát becslések, előrejelzések, ajánlások vagy döntések készítése érdekében, mégpedig a hagyományos statisztikai, matematikai, ökonometria vagy pénzügyi módszereken túlmutató módon. Ez magában foglalja az alábbiakban felsorolt valamennyi MI-kategóriát, valamint azok különböző változatait, például: Generatív mesterséges intelligencia, agentikus mesterséges intelligencia, nagy nyelvi modellek, általános célú MI-modellek stb.

A Mesterséges intelligencia kategóriái közé tartoznak a következők:

- o **Statikus MI:** Olyan MI-technikák, melyeket manuálisan, offline módon tanítanak be, vagy melyek paramétereit explicit módon programozzák be, majd becslések, előrejelzések, ajánlások készítésére vagy döntések meghozására használják.
- o **Dinamikus MI:** Olyan megoldások, melyek a „Statikus MI-vel” ellentétben időszakosan, automatikusan, az éles környezetben újratanulják a paramétereiket.
- o **Automatikus MI:** Olyan „Dinamikus MI-n” alapuló megoldások, melyek képesek automatikusan módosítani alapvető szerkezetüket (pl. hiperparamétereket, bemeneti változókat).
- o **Kognitív MI:** Olyan megoldások, melyek képesek az önálló döntéshozásra és az annak megfelelő cselekvésre, még olyan ügyekben is, amelyekre nem lettek kifejezetten betanítva.

A **Gépi tanulás (ML)** a mesterséges intelligenciák körébe tartozik, és reprezentációkat vagy következtetéseket von le adatokból anélkül, hogy minden paraméterreprezentáció vagy számítási lépés explicit módon programozva lenne. Ilyen megoldások például a Véletlen erdők és a Neurális hálózatokon alapuló megközelítések. Nem a Gépi tanulás részhalmazába tartozó MI-megoldások például az olyan technikák, mint a fuzzy logika és a természetes nyelvi feldolgozás komplex függőségelemző technikái.

Üzleti tevékenységért felelős személy (BAO): a Citi azon alkalmazottja, aki bizonyos a beszállítói kapcsolatokhoz kötődő tevékenységek elvégzéséért és azok aktív irányításáért felelős.

Üzletszerző: a Citi által megbízott Beszállító, aki a Citi nevében új üzleti lehetőségeket azonosít vagy meglévő ügyfélkapcsolatokat kezel.

Üzleti ajándék: minden olyan értékkel bíró dolog (az Üzleti szórakoztatáson kívül), melyet egy Citi alkalmazott ad vagy kap a Citi vagy egy külső fél üzleti tevékenységével kapcsolatban, általában a 25 USD vagy annál alacsonyabb értékű tárgyak kivételével.

Citi-információ: olyan információ, mely a Citi tulajdonát képezi, illetve melyet a Citi köteles védeni annak tárolása, feldolgozása, továbbítása vagy megsemmisítése során, legyen akár digitális, akár nem digitális formátumban.

A Citi-információk besorolásai a következők:

Bizalmas: olyan Citi-vállalkozásokra és/vagy kapcsolt felekre vonatkozó információk, amelyek nem hivatkoznak egyénekre, és magas szintű védelmet igényelnek. Ezen információk bizalmas jellegének, integritásának vagy elérhetőségének veszélyeztetése súlyos hatással lehet a Citi működésére, pénzügyi helyzetére, franchise-ára vagy vállalati ügyfeleire.

Személyazonosításra alkalmas bizalmas adatok: olyan személyes adatok egy adott egyénről, melyek elősegíthetik az adott egyénnel szembeni jogellenes tevékenységek, például személyazonosság-lopás, hitelcsalás vagy egyéb pénzügyi csalás elkövetését. Ezen információk bizalmas jellegének, integritásának vagy elérhetőségének veszélyeztetése jelentős hatással lehet az egyén(ek)re, beleértve többek között a pénzügyi veszteséget vagy a csalást.

- o Azon személyes adatelemek, amelyek más személyes adatokkal kombinálva személyazonosításra alkalmas bizalmas adatokat alkotnak, többek között az egyén neve vagy kapcsolattartási adatai (cím, telefonszám vagy e-mail-cím) a következőkkel kombinálva:
 - Tranzakciós adatelemek, amelyek pénzmozgásokat eredményezhetnek, vagy felhasználhatók személyazonosság-lopás vagy csalás elkövetésére, például:
 - Hitelkártya/betéti kártya száma.
 - Kártyaellenőrzési érték (CVV) vagy PIN-kód
 - Hiteljelentés adatai (hitelpontszám)
 - Teljes születési dátum
 - A munkavállaló teljesítményére (értékelés/visszajelzés) vagy juttatásaira vonatkozó információk
 - Videófelvételek, beleértve a CCTV- és ATM-felvételeket
- Bizonyos személyes adatelemek önmagukban is személyazonosításra alkalmas bizalmas adatoknak minősülnek:
 - o Az Egyesült Államokban használt társadalombiztosítási szám vagy a kormány által kibocsátott azonosítószám (mely használat és/vagy jogi védett állapot szempontjából az Egyesült Államokban használt társadalombiztosítási számmal azonos módon használható), az útlevél száma, a jogosítvány száma vagy egy egyén adóazonosító száma

Belső: olyan nem egyénre vonatkozó információk, melyek üzleti célt szolgálnak, és mérsékelt szintű védelmet igényelnek. Ezen információk bizalmas jellegének, integritásának vagy elérhetőségének veszélyeztetése **korlátozott hatással** lehet egy csapatra vagy egy munkacsoportra.

- o **Személyazonosításra alkalmas adat (PII):** Minden olyan személyes adat, mely:
 - Beazonosít egy egyént vagy háztartást, vagy felhasználható annak azonosítására (például név, aláírás, cím, egyedi nemzeti azonosító, mint például a társadalombiztosítási szám, illetve a lakcímgazolás száma, a születési dátum vagy a jogosítvány száma).
 - Kapcsolódik, ismertet, összeköttetésbe hozható vagy észszerűen összefüggésbe hozható (közvetlen vagy közvetett módon) egy egyénnel vagy háztartással;
 - Felhasználható egy egyén azonosítására vagy a fiókjához való hozzáférés biztosítására (például
 - felhasználónév, e-mail-cím, jelszó, PIN-kód, azonosítószám, biztonsági kérdések válaszai); vagy kapcsolódik egy adott egyénhez és érzékenynek minősülhet (mint például a személyes orvosi vagy egészségügyi adatok, a fiók száma, a fiók értéke).
 - A személyes információk közé tartoznak a védett egészségügyi információk (az Egyesült Államok egészségbiztosítás hordozhatóságáról és elszámolási kötelezettségéről szóló törvény meghatározása szerint), az érzékeny személyes információk és a hitelinformációk (a különböző adatvédelmi/adatbiztonsági és banki titoktartási törvények meghatározása szerint).

Nyilvános: olyan információ, amely szabadon közzétehető a Citi kívül, vagy amely kifejezetten nyilvános felhasználás célját szolgálja, mint például a Citi sajtóközleményei vagy az újságokban a Citiről megjelenő cikkek.

Korlátozott hozzáférésű: olyan kizárólag bizonyos személyek vagy csoportok által használható információ, amelyek a Citi vagy leányvállalatai számára a legérzékenyebbek, és a legmagasabb szintű védelmet igénylik. Ezen információk bizalmas jellegének, integritásának vagy elérhetőségének veszélyeztetése **komoly (cégszintű, több régióra, ill. több szektorra kiterjedő) hatással** lehet a Citi működésére, pénzügyi helyzetére, franchise-ára vagy vállalati ügyfeleire.

- o **Bizalmas, személyazonosításra alkalmas személyes adatok (Bizalmas PII):** olyan személyes adatok amelyeket speciális törvények további védelmet igénylő adatokként jelölnek meg, és amelyek potenciálisan felhasználhatók egy egyén jogellenes megkülönböztetésére, illetve más módon méltánytalanság vagy kár előidézésére. Ezen információk bizalmas jellegének, integritásának vagy elérhetőségének veszélyeztetése jelentős hatással lehet az egyénre (beleértve többek között a pénzügyi veszteséget, a csalást vagy a diszkriminatív hatást).
- Kifejezetten a következőkre vonatkozó adatok: faji, vallási, vallási vagy filozófiai meggyőződés, etnikai hovatartozás, politikai hovatartozás vagy vélemény, szakszervezeti tagság, bűnügyi háttérinformáció vagy bűncselekmények, genetikai adatok, biometrikus adatok, vagy az egyén szexuális irányultságára vagy tevékenységére vonatkozó adatok.
- o Személyes egészségügyi adatok (PHI), amelyek információkat tartalmaznak az illető egészségügyi előtörténetével, illetve mentális vagy fizikai állapotával kapcsolatban.

Ügyfél: a Citi bármely ügyfele vagy vevője, amely lehet többek között egyén (azaz magánszemély), vállalat, intézmény, szervezet és jogi személy.

Felhőregió: egy olyan fizikai hely, ahol a felhőszolgáltató adatközpont(ka)t csoportosít egybe.

Kommunikációs eszközök, rendszerek és szolgáltatások közé tartozik minden olyan hardver, szoftver vagy alkalmazás, amely a Citi üzletvitelével kapcsolatos írott, hang- vagy videóalapú elektronikus kommunikáció továbbítása során használatos. Az eComm csatornák közé tartoznak többek között: számítógépek, laptopok, táblagépek, mobil eszközök és mobiltelefonok, beleértve a „saját eszköz használatát” (BYOD), a BlackBerry, a telefon, a faxszolgáltatások, az intranet- és internet-hozzáférés, a Wi-Fi-szolgáltatások, az e-mail-szolgáltatások, az azonnali üzenetküldő szolgáltatások (például Microsoft Lync, Skype és Bloomberg), a beágyazott kommunikációs funkciókkal rendelkező webhelyek és alkalmazások, a videokonferenciára vagy együttműködésre szolgáló platformok (például Zoom és Microsoft Teams), valamint a közösségi média szolgáltatások, az interaktív információmegosztási szolgáltatások, a harmadik fél által biztosított csevegőszobák, az elektronikus hirdetőtáblák és a blogok.

Tartalom: a Citi bizalmas információi és bármely más olyan adat, jelentés, statisztika vagy információ, amelyet (a) a Citi vagy annak Leányvállalatai, illetve azok vevői, ügyfelei vagy szolgáltatói közvetlenül vagy közvetve a Beszállító rendelkezésére bocsátottak vagy tettek elérhetővé számára, (b) a Szolgáltatásokon keresztül hoztak létre, állítottak elő, vagy (c) a fentiek bármelyikéből származtattak.

Szerződés: írott, két vagy több fél által aláírt jogi dokumentum, amely egy ajánlatot, vállalást, ellenszolgáltatást, a felek kötelezettségeit és a cél jogszerűségét foglalja magában. Szerződések lehetnek például a termékekre és szolgáltatásokra vonatkozó keretmegállapodások, a feladatleírások/munkamegrendelések, a módosítások és kiegészítések, az ütemtervek, a megrendelések vagy bármely más írásos dokumentum, amelyet a Citi vállalat és a Beszállító ír alá. A Titoktartási megállapodás (NDA) szintén Szerződésnek minősül jelen Követelmények alkalmazásában

Hozzáférés-megtagadási (DOA) teszt: annak ellenőrzésére szolgál, hogy a Beszállító rendelkezik-e megfelelő személyi erőforrásokkal és támogatással azoknak a Citi üzleti folyamatokhoz, amelyek a meghatározott RTO-n belül helyreállíthatók.

Szolgáltatásmegtagadási (DOS) teszt: annak ellenőrzésére szolgál, hogy a Beszállító alkalmazása és a Citi üzleti folyamatait támogató infrastruktúra-elemek a meghatározott RTO-n belül helyreállíthatók-e.

„Letétbe helyezett anyagok”: a következő (i)-(vi) alpontokat jelenti együttesen, és kiterjed a Citinek a Citi-környezetben való működtetésre engedélyezett adott szoftverekre, illetve a Beszállító által a Citinek nyújtott Hosztolt szolgáltatásokra használt anyagokra:

- (i) A Citivel kötött vonatkozó megállapodásban meghatározott licencelt szoftver vagy Hosztolt szolgáltatás fejlesztéséhez, működtetéséhez, karbantartásához és támogatásához használt szoftver Forráskódjának pontos másodpéldánya (és az ilyen szoftverek vagy Hosztolt szolgáltatások összes későbbi verziója), valamint a szoftverhez tartozó összes Dokumentáció (függetlenül attól, hogy a Citi már rendelkezik-e a Forráskód egyes részeinek másolatával) („**Letétbe helyezett forráskód**”);
- (ii) Forráskód bármely olyan harmadik féltől származó szoftverhez, mely tekintetében a Beszállító az engedélyezett szoftver vagy Hosztolt szolgáltatás fejlesztésére, üzemeltetésére, karbantartására és támogatására jogosult;
- (iii) Egy engedélyezett példány az olyan szoftvereszközökből, mint például a hibakeresők, assemblerek és fordítók, melyek szükségesek a Letétbe helyezett anyagok részét képező Forráskód futtatható formátumba konvertálásához, illetve a szoftver vagy a Hosztolt szolgáltatások működtetéséhez, karbantartásához és támogatásához;
- (iv) Amennyiben a fentiekben még nem szerepel, bármely olyan Dokumentáció, amely a következőket tartalmazza: (A) a Letétbe helyezett anyagok általános leírása és

- működése; (B) architektúra és alapvető programfunkciók; (C) adatfolyam-információk; (D) részletes memóriatérkép és lista; (E) bemeneti/kimeneti porttérképek; és (F) olyan egyéb információk, amelyek lehetővé tennék egy az adott programozási nyelvben vagy nyelvekben jártas átlagos képességű programozó számára a Letétbe helyezett anyagokban található Forráskód használatát és módosítását;
- (v) Minden egyéb a szoftverrel vagy a Hosztolt szolgáltatással kapcsolatos technikai információ, melyről észszerűen feltételezhető, hogy szükség van a szoftver vagy Hosztolt szolgáltatás Citi vagy a Citi nevében eljáró illetékes harmadik fél általi használathoz, üzemeltetéshez, módosításhoz és fejlesztéshez; és
- (vi) A szoftverrel vagy a Hosztolt szolgáltatásokkal kapcsolatban használt összes harmadik féltől származó szoftver és technológia listája, mely észszerű részletességgel leírja azok a kérdéses szoftverben való felhasználását, valamint az adott szoftver vagy technológia szolgáltatójának elérhetőségeit. A Citi tudomásul veszi és elfogadja, hogy a Letétbe helyezett anyagok a (ii) alszakaszban foglaltakon kívül nem tartalmaznak harmadik féltől származó forráskódot; és
- (vii) a Hosztolt szolgáltatásokkal kapcsolatban:
- a felhőben üzemeltetett éles környezet kis méretű másolata, illetve a környezetre jellemző felhőalapú erőforrások és minden egyéb olyan információ, amely a Citi éles környezetének reprodukálásához szükséges, beleértve (többek között) az alábbiakat: infrastruktúra-elemek, például infrastruktúrakód, terraform szkriptek, felhőalapú erőforrások, CloudFormation-sablonok, konfigurációs fájlok, felhő ügyfelek, felhő-előfizetések, virtuálisgép-lemezképek, docker-képfájlok és a szoftver infrastruktúrájának forráskódja; valamint
 - a szoftverben tárolt Citi-adatok másolata.

Elektronikus kommunikáció: a Személyzet által elektronikus módon, vezetékes vagy vezetékek nélküli jelek útján továbbított, fogadott vagy felhasznált üzenetek és információk. Az Elektronikus kommunikáció magában foglalja többek között a szöveges üzeneteket, az e-maileket, a társközi és azonnali üzeneteket, a blogbejegyzéseket, a közösségi médiában közzétett bejegyzéseket, az üzenetküldő alkalmazásokon, például a WhatsAppon, a WeChaten, a Line-on, a Signalon és a Viberen keresztül küldött üzeneteket, valamint a mellékleteket, a képernyőképeket, a rögzített audio- és videófájlokat, az élő hangot és videót, valamint az Elektronikus kommunikációs eszközökön, rendszereken és szolgáltatásokon keresztül létrehozott, fogadott, letöltött, tárolt, továbbított, törölt és felhasznált fájlokat.

Funkcionális azonosítók: általános azonosítók, például ADMIN vagy ROOT, melyeket egy személy vagy folyamat használ egy biztonsági rendszer eléréséhez. A személyazonosság és hozzáférés kezelése (IAM) művelet egyik kulcsfontosságú kezdeményezése annak biztosítása, hogy a Citi rendelkezzen konkrét, meghatározott ellenőrző eszközökkel a funkcionális azonosítók használatára vonatkozó kockázatok elleni védekezés érdekében.

Franchise szempontjából kritikus folyamatok/alkalmazások (FCA): olyan folyamatok/alkalmazások, melyeket a Citi a franchise szempontjából kritikus üzleti funkcióinak sikeres teljesítéséhez elengedhetetlennek minősített.

Csalás: szándékos cselekmény, téves állítás vagy mulasztás, melynek célja mások megtévesztése, és melynek eredményeként vagy veszteség éri az áldozatot, vagy az elkövető nyereségre tesz szert.

Hosztolt szolgáltatás: minden a Beszállító által a Hosztolt szolgáltatások biztosításához Telepített alkalmazás, illetve kezelt vagy használt létesítmény és környezet, a Hosztolt

szolgáltatásokhoz telepített vagy felhasznált összes alkalmazás és egyéb szoftver, adatbázis, weboldal, szerver, hardver, hálózat, telekommunikációs és egyéb berendezés, illetve egyéb technológia, minden esetben az összes Frissítést és Támogatási szolgáltatást is beleértve, de kizárva az összes Tartalmat és a Citi-Rendszereket.

Személyazonosság-ellenőrző adatok (IVD): biztonsági kérdések (SQ) vagy tudásalapú hitelesítési (KBA) kérdések. A biztonsági kérdéseket általában az alkalmazás határozza meg, és a végfelhasználónak kell válaszolnia rájuk. Ilyen például az édesanya leánykori neve, születési helye, kedvenc foglaltja stb. Mindkét kérdéstípust hitelesítési adatként kell kezelni.

Információbiztonság (IS): olyan állapot, melyben egy számítógép vagy számítógépes rendszer védve van a jogosulatlan hozzáféréstől vagy támadástól, úgy, hogy (a) a számítógép vagy számítógépes rendszer továbbra is elérhető és működőképes marad; (b) a számítógép vagy számítógépes rendszer integritása megmarad; és (c) a számítógépen vagy számítógépes rendszeren tárolt, feldolgozott vagy továbbított információk integritása és bizalmassága megmarad.

Információbiztonsági fenyegetés: olyan (ismert vagy gyanított) cselekedet vagy tevékenység, melyet számítógépen vagy számítógépes rendszeren vagy ezeken keresztül hajtanak végre, és mely veszélyeztetheti vagy hátrányosan befolyásolhatja az adott vagy egy másik számítógép vagy számítógépes rendszer információbiztonságát.

Információbiztonsági sebezhetőség: a számítógépen vagy a számítógépes rendszeren lévő bármely olyan biztonsági rés, amelyet egy vagy több információbiztonsági fenyegetés kihasználhat.

Nem ügyfél/nem bevételt generáló tevékenységek: üzleti szempontból kritikus, de bevételt generáló tevékenységekhez nem kapcsolódó tevékenységek; ide tartoznak a jogi, felügyeleti, szabályozási és üzletmenet-folytonossági tevékenységek.

Titoktartási megállapodás (NDA): egy olyan megállapodás a Citi és a Beszállító között, amelynek megfelelően az információ cseréjét, felhasználását és közzétételét a megállapodás feltételei szabályozzák.

Nyílt forráskódú szoftver: olyan forráskód vagy lefordított számítógépes program, amely esetében a forráskód a nyilvánosság számára elérhető, és az eredeti formájához képest módosítható.

Személyzet: a Beszállító és annak leányvállalatai, igazgatói, tisztségviselői, alkalmazottai, ügynökei, könyvvizsgálói, tanácsadói, szolgáltatói és vállalkozói (kivéve a Citi személyzetét), akár egyértelműen megnevezve, akár a kontextusból származtatva. A Beszállító személyzete magában foglalja bármely Alvállalkozó igazgatóit, tisztségviselőit, alkalmazottait, ügynökeit, könyvvizsgálóit, tanácsadóit vagy egyéb képviselőit is.

Nyilvántartásjegyzék: egy részletes jegyzék, amely tartalmazza a Citi nyilvántartások típusát, helyét, dátumát stb., és amelynek vezetése elengedhetetlen ahhoz, hogy egy vállalat megfelelően kezelhesse a nyilvántartásait az információk életciklusa során.

Információmegőrzési rendelkezés: Nyilvántartásra és Információra vonatkozó követelmény, mely az illetékes hatóság általi feloldásáig felfüggeszti a módosítást és megsemmisítést.

Helyreállítási kapacitás: a Beszállító termékeinek és szolgáltatásainak volumene, mennyisége vagy teljesítési sebessége, a termékek és szolgáltatások normál teljesítésének százalékában kifejezve.

Helyreállítási időtartam: az a naptári napokban meghatározott maximális időtartam, mely alatt a Beszállító helyreállítási üzemmódban képes fenntartani működését.

Helyreállítási pontra vonatkozó célkitűzés: az az órában megadott múltbeli időpont, ameddig az adatokat helyre kell állítani egy üzleti tevékenység megszakadása után. Ez egy maximális célzott időtartam, amely alatt az adatok elveszhetnek egy informatikai szolgáltatást érintő jelentős incidens bekövetkezése esetén. Az RPO kizárólag azt a maximális időtartamot méri, amely alatt az adatok elveszhetnek egy IT-szolgáltatást érintő jelentős incidens bekövetkezése esetén. Ez nem közvetlen mérőszáma annak, hogy mennyi adat veszhet el, pl. az előző napi feldolgozás végére.

Helyreállítási időcél: a szolgáltatásmegszakadás és a termékek és szolgáltatások helyreállítása között eltelt időtartam, órákban mérve.

A „**Megszűnési esemény**” az alábbi egy vagy több események valamelyikét jelenti:

- (i) a Beszállító (A) fizetéseképtelenné válik, vagy elismeri, hogy általánosságban képtelen tartozásait esedékességükkor megfizetni; (B) önként vagy akaratán kívül bármilyen belföldi vagy külföldi csődeljárás vagy fizetéseképtelenségi eljárás alá kerül, melyet nem függesztenek fel teljesen hét (7) munkanapon belül, illetve nem utasítanak el vagy szüntetnek meg a bejelentést követő negyvenöt (45) napon belül; (C) általános engedményezést tesz hitelezők javára; vagy (D) bármely illetékes bíróság határozata alapján felszámolót, vagyonkezelőt, letétkezelőt vagy hasonló végrehajtót neveztek ki vagyonának vagy üzleti tevékenységének bármely jelentős részének átvételére vagy értékesítésére.

Erőforrás-gazdálkodási szervezet (RMO): a Citi globális, végpontok közötti erőforrás-gazdálkodásáért felelős, beleértve a stratégiai beszerzést, a beszerzéstől a fizetésig terjedő műveleteket, a személyzeti hivatalt és a beszállítói menedzsment keretrendszerét.

RMO forrásbeszerzési menedzser: az erőforrás-menedzsment szervezeten (RMO) belül az a személy, aki felelős a szerződéses üzleti feltételek, a követelmények és az árképzés megtárgyalásáért, ideértve

az RFP-eket és az egyéb Beszállító-kiválasztási tevékenységeket, valamint a szerződés feltételeinek és a pénzügyi értékelés akkreditációs követelményeinek adminisztrációjáért.

Súlyos vagy katasztrofális káros hatás: egy egyénre nézve azt jelenti, hogy a hatás észszerűen jelentős káros hatással járhat az adott egyénre nézve, ideértve a pénzügyi veszteséget, a munkahely elvesztését, illetve a munkába állás ellehetetlenítését vagy megnehezítését, az emberi jogok terén történő veszteségeket, személyes vagy nyilvános megalázást vagy a jogtalan börtönbüntetést.

Alvállalkozó: Az alvállalkozó egy olyan negyedik fél (magán- vagy jogi személy), akit egy harmadik fél fogadott fel, hogy a Citi által a harmadik féllel szerződött szolgáltatások vagy tevékenységek egy részét vagy egészét elvégezze.

Útmutatás:

K1: Le kell jelenteni a harmadik fél valamennyi alvállalkozóját?

V1: Kizárólag az elvégzett szolgáltatáshoz kapcsolódó alvállalkozókat kell lejelenteni. Az alvállalkozó által végzett szolgáltatások vagy tevékenységek közé többek között a következők tartoznak:

* Olyan alvállalkozó, aki olyan technológiai vagy szoftverszolgáltatásokat nyújt, amelyek közvetlenül vagy közvetve támogatják a Citi által a harmadik féllel szerződött szolgáltatásokat/tevékenységeket; vagy

* Olyan alvállalkozó, akinek a szolgáltatásai közé tartozik a bizalmas vagy magasabb szintű Citi információkhoz való hozzáférés; vagy

* Olyan alvállalkozó, aki közvetlen vagy közvetett kapcsolatban áll a Citi bármely meglévő/potenciális Ügyfelével; vagy

* Olyan alvállalkozó, aki kíséret nélkül végzi a Citi dokumentumainak megsemmisítését vagy archiválását a Citi bármely létesítményén belül vagy kívül; vagy

* Olyan alvállalkozó, aki az alapvető banki funkciók vagy szolgáltatások (pl. kifizetések, begyűjtés, hitelezés) támogatásában vesz részt.

Beszállító: Jelen „Beszállítókra vonatkozó Citi-követelmények” című dokumentum alkalmazásában a „Beszállító” kizárólag olyan Külső harmadik felet jelent, aki üzleti megállapodást kötött egy Citi-vállalattal, hogy annak közvetlenül termékeket vagy szolgáltatásokat biztosítson, vagy azt üzleti céljainak elérésében támogassa. A Külső harmadik fél a Citihez nem tartozó entitást jelent. A Beszállítók lehetnek egyben egy Citi-vállalat kliensei vagy ügyfelei, illetve támogathatják a Citi ügyfeleivel és vásárlóival folytatott interakcióit is; azonban jelen dokumentum hatályán belül a kizárólag Citi-ügyfél státusz alapján kötött megállapodások nem minősülnek beszállítói kapcsolatnak.

Átmeneti információk: Nyilvántartásnak minősül az információ végleges és legteljesebb változata, amelynek megőrzésére a Citi jogszabályi, hatósági vagy jóváhagyott üzleti okból köteles. Minden egyéb információ „Átmeneti információnak” minősül.