КСЕЛЛ АҚ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ЖӨНІНДЕГІ ДИРЕКТИВАЛАР

1 Сипаттамасы

Осы құжат («Қауіпсіздікті қамтамасыз ету жөніндегі директивалар») Жеткізушілерге (төмендегі анықтамаға сәйкес), сондай-ақ Kcell АҚ-ның белгілі бір іскерлік серіктестеріне қолданылатын қауіпсіздік жөніндегі талаптарды сипаттайды. Қауіпсіздік жөніндегі қосымша талаптар жекелеген жағдайларда тартылған тараптардың келісімі болған кезде қолданылуы мүмкін.

2 Анықтамалар

1. **«Келісім»** Kcell АҚ мен Жеткізуші немесе оған сәйкес Қауіпсіздік жөніндегі директивалар қолданылатын және олар бір бөлігі болып табылатын басқа да Kcell АҚ бизнес-серіктесі арасындағы келісімді білдіреді.
2. **«Kcell деректері»** Kcell немесе Kcell атынан әрекет ететін тұлға жеткізушіге беретін деректерді немесе басқа ақпаратты, сондай-ақ Жеткізушінің осындай деректерді өңдеу нәтижесін білдіреді.
3. **«Ақпаратты өңдеу құралдары»** ақпаратты өңдеу жөніндегі кез келген жүйелерді, қызметтерді немесе инфрақұрылымды немесе олар орналастырылатын жеке үй-жайларды білдіреді.
4. **«Есеп жүргізу»** ақпаратты немесе оқиғаларды әдетте, осындай ақпарат немесе оқиға туындайтын реттілікте есепке алу жүйесінде жазуды білдіреді.
5. **«Дербес деректер»** қолданылатын міндетті ұлттық заңнаманы ескере отырып, ЕО 95/46/ЕО директивасына (немесе қолданыстағы осыған ұқсас заңнамаға) сәйкес айқындалған мәнге ие.
6. **«Қызметтер»** Тараптар арасындағы Келісімде келтірілген анықтамаға сәйкес Kcell компаниясының Жеткізушісі немесе Жеткізуші атынан әрекет ететін тұлға көрсететін қызметтерді білдіреді.
7. **«Жеткізуші»** Kcell компаниясына жеткізуді жүзеге асыратын контрагентті білдіреді; сондай-ақ «Сатушы», «Серіктес» деп аталады немесе тиісті Келісімде айқындалған өзге де баламалы атауы болады.
8. **«Жеткізуші персоналы»** Жеткізуші атынан жұмыс істейтін кез келген тұлғаны (қызметкерлер, консультанттар, қосалқы мердігерлер және т.б.) білдіреді.
9. **«Қауіпсіздікті бақылау»** IT-жүйелер қауіпсіздігінің қажетті техникалық және сапалық параметрлерін қолдауға мүмкіндік беретін қарсы іс-қимылдың техникалық шараларын, ұйымдық құрылымды немесе процесті білдіреді.
10. **«Ақпараттық қауіпсіздік оқиғасы»** ұйымның экономикалық қызметінің нашарлауы мен оның қауіпсіздігіне қатер төндіруінің жоғары ықтималдығын тудыратын қауіпсіздіктің қалаусыз немесе күтпеген оқиғаларының бірлі-жарым немесе сериясын білдіреді.

«Стратегиялық тауарлар» және **«Стратегиялық қызметтер»** Kcell компаниясы стратегиялық ретінде айқындаған кез келген өнімді немесе Қызметтерді білдіреді. Стратегиялық тауарлар/қызметтер тиісті Келісімде нақты көрсетілуі тиіс.

3 Қолданылу аясы

Қауіпсіздікті қамтамасыз ету жөніндегі директивалар келесі жағдайларда қолданылады:

1. Жеткізушінің Kcell деректерін өңдеуі;
2. Жеткізушінің Kcell аумағында болуы;
3. Жеткізушіге Kcell желілері мен IT-жүйелеріне, оның ішінде қашықтықтан қол жеткізу арқылы қол жеткізуді ұсыну;
4. Жеткізушінің Kcell ақпаратты өңдеу жабдығын пайдалануы;
5. Kcell компаниясы Жеткізушіні тиісті шарт негізінде Стратегиялық тауарлар және/немесе Стратегиялық қызметтер провайдері ретінде тартқан жағдайында.

4 Жеткізушінің толық жауапкершілігі

1. Жеткізуші оның персоналының Қауіпсіздікті қамтамасыз ету жөніндегі директиваны сақтауына толық жауапты болады.

2. Жеткізуші Kcell үшін кез келген тапсырманы орындау алдында Қауіпсіздік жөніндегі директиваларға сәйкестікті қамтамасыз ету үшін қажетті шараларды жүзеге асыруға міндетті.
3. Kcell талабы бойынша Жеткізуші Қауіпсіздік жөніндегі директиваның сақталуы қалай қамтамасыз етілетіні және Жеткізушінің Қауіпсіздік жөніндегі директиваның талаптарына сәйкестігін қамтамасыз ету үшін қандай шаралар қолданғаны туралы Kcell-ге хабарлауға міндетті.
4. Жеткізуші кез келген Қауіпсіздік инциденттері (Дербес деректерді өңдеуге байланысты инциденттерді қоса алғанда, бірақ шектелмей) туралы Kcell supplier@kcell.kz электрондық мекенжайы бойынша қысқа мерзімде, бірақ Қауіпсіздік инциденті анықталғаннан кейін кемінде 24 сағат ішінде хабардар етуге міндетті. Төмендегі инциденттерді басқару жөніндегі ақпаратты қараңыз.
5. Жеткізуші Kcell Деректерін кез келген өңдеу Қауіпсіздік жөніндегі директиваларға қатаң сәйкестікте жүзеге асырылатынына кепілдік береді.
6. Жеткізуші кез келген Kcell Деректерін және олардың көшірмелерін қайтаруға немесе жоюға міндетті (Kcell қарауына қарай). Жеткізуші Келісім тоқтатылған жағдайда немесе Kcell талабы бойынша осы талаптың орындалуын жазбаша растауды Kcell-ге ұсынуға міндетті.

Жеткізуші Kcell тарапынан алдын ала жазбаша мақұлдаусыз Келісімді бұза отырып, Kcell Деректеріне (оның ішінде жаңа, кеңейтілген, жаңартылған, ұзақ немесе нақты уақыт режимінде желіге қол жеткізудің өзге де нысандары) үшінші тұлғаларға қол жеткізуді ұсынбауы тиіс.

5. Қауіпсіздік талаптары

5.1 Тәуекелдерді басқару

1. Жеткізуші қауіпсіздік саласындағы тәуекелдерді анықтауға және осындай тәуекелдерді бақылау және азайту үшін қажетті шаралар қолдануға міндетті.
2. Жеткізушінің өз қызметі шеңберінде тәуекелдерді өңдеу бойынша құжатпен ресімделген процестері мен рәсімдері болуға міндетті.
3. Жеткізуші ақпараттық жүйелермен және ақпаратты өңдеумен, сақтаумен және берумен байланысты тәуекелдерді бағалауды кезең-кезеңмен жүргізуге тиіс.

5.2 Ақпараттық қауіпсіздік саласындағы саясаттар

1. Жеткізушінің әзірленген және құжатпен ресімделген ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ), оның ішінде Жеткізушінің басшылығы бекіткен ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қолданыстағы саясат пен рәсімдер болуы тиіс. Мұндай құжаттар Жеткізушінің ішкі ресурстарында жариялануға және Жеткізушінің тиісті Персоналының назарына жеткізілуге тиіс.
2. Жеткізуші қауіпсіздік саласындағы саясат пен рәсімдерді кезең-кезеңмен қайта қарауға және қажет болған жағдайда олардың Қауіпсіздік директиваларына сәйкестігін қамтамасыз ету мақсатында оларды жаңартуға тиіс.

5.3 Ақпараттық қауіпсіздікті ұйымдастыру

1. Жеткізуші өз ұйымы шеңберінде қауіпсіздікті қамтамасыз ету жөніндегі рөлдер мен міндеттерді анықтауға және құжатпен бекітуге тиіс.
2. Жеткізуші Қауіпсіздік жөніндегі директиваларға сәйкес қауіпсіздік шараларын жүзеге асыруға жалпы жауапты болатын және Kcell қауіпсіздік қызметінің қызметкерлері үшін байланыс тұлғасы болып табылатын қауіпсіздік саласында тиісті құзыреті бар кем дегенде бір адамды тағайындауға тиіс.

5.4 Персоналдың қауіпсіздігін қамтамасыз ету

1. Жеткізуші оның Персоналы Келісімде белгіленген құпиялылық деңгейіне сәйкес ақпаратты өңдеуді жүзеге асыратынын қамтамасыз етуге тиіс.
2. Жеткізуші Келісімге сәйкес ақпаратты, құралдар мен жүйелерді рұқсат етілген пайдалану (оның ішінде мән-жайларға байланысты, пайдалануды шектеу) туралы өз Персоналының хабардар болуын қамтамасыз етуге тиіс. Kcell Жеткізушінің әрбір қызметкерінен олардың танысқандығы, Қауіпсіздік жөніндегі директиваларды түсінетіндігі және сақтауға және ақпаратты, құралдар мен жүйелерді рұқсат етілген мақсаттарда ғана пайдалануға міндеттенетіндігі туралы тиісті қолхат беруді талап етуге құқылы.
3. Жеткізуші Келісім бойынша тапсырманы орындауға тартылған оның кез келген қызметкерінің сенімді болып табылатынына, белгіленген қауіпсіздік өлшемдеріне жауап беретініне және тиісті скринингтен және жеке деректерді тексеруден өткеніне кепілдік беруге тиіс.
4. Жеткізуші Kcell-ге Жеткізушінің жауапкершілігімен жұмыс істейтін, шарт бойынша қызмет көрсететін барлық қызметкерлердің, консультанттардың, мердігерлердің және Жеткізушінің басқа да тұлғаларының тізімін алдын ала ұсынуы тиіс. Тізімде аты, жеке коды және телефон нөмірі және электрондық пошта мекенжайы («Өнім беруші персоналының тізімі») сияқты байланыс ақпараты болуы тиіс және Жеткізуші шарттың қолданылу мерзімі ішінде кез келген уақытта тізімге өзгерістер енгізуі тиіс. Жеткізуші Персоналының Тізімі Kcell жүйелеріне немесе Kcell үй-жайларына қол жеткізу құқықтарының шындығын тексеру үшін сілтеме ретінде тексерулерді жүзеге асыру кезінде кез келген уақытта пайдаланылуы мүмкін.

5. Жеткізуші қауіпсіздік үшін жауапты Жеткізуші Персоналының қауіпсіздікті қамтамасыз ету жөніндегі өз міндеттерін тиісінше жүзеге асыру үшін қажетті оқытудан өтуін қамтамасыз етуге тиіс.

6. Жеткізуші Жеткізушінің тиісті персоналы үшін қауіпсіздік бойынша тұрақты оқытуды жүргізуді қамтамасыз етуі тиіс. Мұндай оқыту шектеусіз мыналарды қамтуы тиіс:

   a. Клиенттің ақпараттық қауіпсіздігін қалай қамтамасыз ету (яғни ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қорғау);

   b. Клиенттердің ақпараттары мен жүйелерін қорғау үшін неге ақпараттық қауіпсіздік қажет;

   c. Қауіпсіздікке төнетін қауіп-қатерлердің жалпы түрлері (мысалы, жеке деректерді ұрлау, зиянды бағдарламалар, хакерлер, ақпараттың таралып кетуі және ішкі қауіп-қатер);

   d. Ақпараттық қауіпсіздік саясатын сақтаудың және тиісті стандарттар/рәсімдерді қолданудың маңыздылығы;

   e. Ақпараттық қауіпсіздік үшін дербес жауапкершілік (мысалы, клиенттің жеке деректерін қорғау, сондай-ақ қауіпсіздікті бұзудың нақты және болжамды жағдайлары туралы ақпарат беру).

7. Жеткізуші Kcell үшін тапсырмаларды орындайтын Жеткізуші Персоналының тапсырмаға байланысты телекоммуникациялық деректер мен бизнес-ақпараттың құпиялылығын сақтау жөніндегі міндеттемелер туралы, сондай-ақ ақпараттың, құралдар мен жүйелердің бекітілген пайдаланылуы туралы хабардар болуын қамтамасыз етуге тиіс. Kcell Жеткізушінің Персоналынан барлық қызметкерлер рұқсат етілген мақсаттарда жүйелер мен құралдарды пайдалану жөніндегі міндеттемелерді түсінетіндігі және сақтауға міндеттенетіндігі туралы қолхат талап етуге құқылы.

5.5 Активтерді басқару

1. Жеткізушінің активтерді басқарудың құжатпен ресімделген және қолданыстағы жүйесі болуы және барлық тиісті активтер мен олардың иелерінің уақтылы есебін жүргізуі тиіс. Ақпараттық активтерге құпия ақпарат, қол жеткізу құқықтары, бағдарламалық қамтамасыз ету және конфигурацион бар IT-жүйелер, резервтік көшірме жасау және/немесе алмалы-салмалы жеткізгіштер кіреді, бірақ олармен шектелмейді.

2. Жеткізуші ақпаратты жіктеудің алдын ала анықталған жүйесіне сәйкес осы сәтте қолданылып жүрген қауіпсіздік стандарттарына сәйкес (ақпарат жеткізгіштерді сақтау, кәдеге жарату және физикалық беруді қоса алғанда) ақпаратты таңбалауға, жүгінуге және қорғауды қамтамасыз етуге міндетті.

5.6 Қол жеткізуді басқару

1. Жеткізушінің объектілерге, сайттарға, желілерге, жүйелерге, қосымшаларға және ақпаратқа/деректерге (физикалық, логикалық және қашықтан қол жеткізуді басқаруды қоса алғанда) қол жеткізуді басқару жөніндегі құжатпен ресімделген және қолданыстағы саясаты, пайдаланушылық қол жеткізу және артықшылықтар беру үшін авторландыру процесі, қол жеткізу құқығын жою жөніндегі рәсімдер болуы және Жеткізуші персоналының қол жеткізу артықшылықтарын қолайлы пайдалануы тиіс.

2. Жеткізушінің қол жеткізу құқығын беру үшін пайдаланушыларды тіркеу/тіркеудің күшін жою бойынша құжатпен ресімделген және қолданыстағы рәсімі болуы тиіс.

3. Жеткізуші қызметтік қажеттілік қағидатын және ең аз артықшылықтар қағидатын негізге ала отырып, қол жеткізудің барлық артықшылықтарын тағайындауға тиіс.

4. Жеткізуші Kcell Деректері бар жүйелермен жұмыс істеу кезінде жоғары артықшылықтары бар жүйелік әкімшілерге немесе басқа да пайдаланушыларға, оның ішінде қашықтықтан қол жеткізуді пайдаланушыларға арналған қатаң (2 факторлық) сәйкестендіру жүйесін пайдалануы тиіс.

5. Жеткізуші оның Персоналының жеке және бірегей сәйкестендіргіші (user ID) болуына кепілдік беруі және пайдаланушылардың түпнұсқалығын растау және кепілдендіру үшін сәйкестендірудің тиісті тәсілін пайдалануы тиіс.

6. Жеткізуші Kcell ақпаратына рұқсаты бар Жеткізушінің Персоналындағы өзгерістер туралы Kcell-ге негізсіз кідіртулерсіз хабарлауға міндетті.

5.7 Криптография

1. Жеткізуші криптографияның құпия және құпия ақпаратқа (мысалы, Дербес деректер) жатқызылған ақпаратқа Kcell ақпаратының құпиялылығын жіктеу схемасына сәйкес төменде егжей-тегжейлі баяндалғандай тиісінше және тиімді қолданылуын қамтамасыз етуі тиіс.

2. Жеткізуші криптографиялық кілттерді қорғауды қамтамасыз етуі тиіс.

5.8 Жеке қауіпсіздік және қоршаған ортаның қауіпсіздігі

1. Жеткізуші Ақпаратты өңдеу құралдарын сыртқы және экологиялық қауіп-қатерлерден, электр сымындағы электрмен жабдықтаудың үзілістерін/ақаулықтарды және энергетикалық жүйелердің істен шығуынан туындаған басқа да бұзушылықтарды қоса алғанда, қорғауды қамтамасыз етуге тиіс. Бұл жерге физикалық периметр және қол жетімділікті қорғау жатады.

2. Жеткізуші Kcell атынан алынған немесе жөнелтілген тауарларды ұрлықтан, алаяқтықтан және бұзудан қорғауы тиіс.

5.8.1 Kcell үй-жайларына және Kcell жалға алған үй-жайларға қол жеткізу

Жеткізушіні Kcell аумағына және мүлкіне (деректерді өңдеу орталығының ғимараттары, кеңсе ғимараттары, техникалық сайттар) жіберу мынадай ережелерді сақтай отырып жүзеге асырылуы тиіс:

1. Тапсырма Келісімге сәйкес орындалған кезде Жеткізуші ұлттық заңнаманың (мысалы, қол жеткізу шектелген аймақтар саласындағы заңнаманың) талаптарын сақтауға міндеттенеді.
2. Kcell үй-жайларында жұмыс істеген кезде Жеткізушінің Персоналында өзімен бірге жеке куәлігі немесе көрнекті жерде келушінің рұқсаты болуға және үнемі алып жүруге міндетті.
3. Тапсырманы орындау аяқталғаннан кейін немесе Жеткізушінің Персоналы басқа міндеттерді шешуге жіберілген жағдайда Жеткізуші осындай өзгеріс туралы Kcell-ге дереу хабарлауға және кілттерді, магниттік кілттерді, куәліктерді, келушілердің рұқсаттамаларын және басқа сәйкестендіру құралдарын қайтаруға немесе бөлуді өзгертуге міндетті.
4. Кілттер немесе магниттік кілттер Жеткізуші Персоналының ішінен белгілі бір қызметкер үшін жеке ресімделуі тиіс және кілттер немесе магниттік кілттер алғандығы туралы қолхатта келтірілген жазбаша ережелерге сәйкес пайдаланылуы тиіс.
5. Kcell кілтінің немесе магниттік кілтінің жоғалғаны туралы ақпарат дереу Kcell назарына жеткізіледі.
6. Kcell аумағында және нысандарында тиісті рұқсатсыз суретке түсіруге тыйым салынады.
7. Тиісті рұқсатсыз Kcell-ге тиесілі тауарларды оның аумағынан шығаруға тыйым салынады.
8. Жеткізуші персоналына Kcell аумағына бөгде адамдарға кіруге рұқсат беруге тыйым салынады.
9. Жеткізуші Персоналы Келісімнің шарттарын орындамаған жағдайда, Kcell Жеткізушіге өз аумағына ұсынудан дереу бас тартуға және талап/талап бойынша негізсіз кідіріссіз қайтару шартымен берілген кілттерді, кілт-карталарды және т.б. қайтаруды талап етуге құқылы.

5.8.2. Kcell үй-жайларына қатысты жалпы ережелер

Жеткізуші персоналы Kcell үй-жайларына қатысты мынадай жалпы ережелерді ұстануы тиіс:

1. Темекі шегуге бөлінген орындарды қоспағанда, Kcell үй-жайларында темекі шегуге тыйым салынады.
2. Kcell үй-жайларында алкогольді немесе есірткіні (ұйғарылған фармацевтикалық препараттардан басқа) тұтынуға тыйым салынады.
3. Алдын ала келісім алмастан Kcell үй-жайларында немесе Kcell аумағындағы тұрғын тіркемелердің немесе ұқсас көлік құралдарының тұрақтарында түнеуге тыйым салынады.
4. Егер тараптар өзгеше белгілемесе, қызметкерлер Kcell аумағындағы аймақтардың ешқайсысын қойма үй-жайлары ретінде пайдалана алмайды.
5. Шартта өзгеше көзделген жағдайларды қоспағанда, компьютерлерді, телефондарды, принтерлерді, факстерді немесе Kcell-ге тиесілі кез келген басқа жабдықты пайдалануға тыйым салынады.
6. Kcell меншігі рұқсатсыз Kcell үй-жайынан жойылмайды.
7. Рұқсатсыз Kcell бөлмелерінде суретке түсіруге тыйым салынады.
8. Егер Жеткізуші орындауға тиіс жұмыстарды жүргізу кезінде шаңдану, шу, діріл немесе өрт туындау қаупі болса, Жеткізуші мұндай жұмыстарды жүзеге асыру үшін алдын ала Kcell рұқсатын алуға міндетті.
9. Өрт дабылы, күзет дабылы және апат туралы хабарлау жүйесі сияқты сигнализация Kcell рұқсатымен ғана ажыратылуы мүмкін. Күзет сигнализациясы жүйесі жұмыстар аяқталғаннан кейін дереу қалпына келтірілуі тиіс. Сигнализация өшірілгенге дейін, уақытта және кейін жүзеге асырылатын рәсімдер мен іс-қимылдар шартта және жергілікті заңдар мен ережелерге сәйкес көрсетілуі тиіс.
10. Жеткізуші жұмыс аймағындағы терезелер мен есіктердің жабық күйде болуына, сондай-ақ үй-жайларға бөгде адамдардың кіру мүмкіндігінің болмауын қамтамасыз етуге жауапты болады.
11. Жеткізушінің персоналы өзінің жұмыс орындарын таза және тәртіпте ұстауы тиіс. Қоқыс пен буып-түю материалдары дереу алынып, Kcell көрсетілген жерге шығарылуы тиіс.
12. Өрт болған жағдайда авариялық жабдықтар немесе эвакуациялау аймағы Жеткізуші қызметі нәтижесінде бұғатталмауы тиіс.
13. Жеткізуші өз персоналы үшін Kcell үй-жайларында жұмыс басталар алдында қауіпсіздік техникасына оқыту жүргізуі тиіс.

5.9 Жедел қауіпсіздік

1. Жеткізушінің бизнес процестерге, Объектілердегі және жүйедегі ақпаратты өңдеу құралдарына өзгерістер енгізу үшін қолданыстағы өзгерістерді басқару жүйесі болуы тиіс. Өзгерістерді басқару жүйесі өзгерістерді енгізу алдындағы тесттер мен шолуларды қамтиды, мысалы: шұғыл өзгерістерді өңдеу рәсімдері; сәтсіз өзгерістерден кейін бастапқы жай-күйіне қайтару жөніндегі рәсімдер; енгізілген өзгерістерді және оларды кім және қашан енгізгенін көрсететін журналдар.

2. Жеткізушінің Kcell пайдасына Келісім бойынша қызметтер/материалдар ұсынуы үшін пайдаланылатын кез келген бағдарламалық қамтамасыз етудің зиянды бағдарламалардан қорғалғанына кепілдік беру үшін Жеткізушінің зиянды бағдарламалардан қорғау жүйесі болуы тиіс.
3. Жеткізуші маңызды ақпараттың резервтік көшірмелерін жасауға, сондай-ақ Kcell-мен келісім бойынша ақпаратты қалпына келтіру мақсатында резервтік көшірмелерді тестілеуді жүргізуге тиіс.
4. Жеткізуші пайдаланушының іс-әрекеттерін, ерекшеліктерді, қателерді және ақпараттық қауіпсіздік оқиғаларын Есепке алуға және мониторингін жүзеге асыруға және оларды үнемі тексеруге міндетті. Бұдан басқа, Жеткізуші Есептік ақпаратты қорғауды және сақтауды (кемінде 6 ай ішінде) қамтамасыз етуге және сұрау салу бойынша мониторинг деректерін Kcell-ге беруге тиіс.
5. Жеткізуші операциялық жүйелер, деректер базалары, қосымшалар сияқты барлық тиісті технологияларға қатысты осалдықтың факторларын белсенді және уақтылы басқаруға тиіс.
6. Жеткізуші операциялық жүйелер, деректер базалары, қосымшалар сияқты барлық тиісті технологиялар үшін қауіпсіздіктің базалық деңгейлерін (қорғанысты күшейту) белгілеуі тиіс.
7. Жеткізуші тестілік және өндірістік орта арасындағы аражігін ажыратуды қамтамасыз етуі тиіс.

5.10 Байланыс қауіпсіздігі

1. Жеткізуші қызмет көрсету деңгейі, желіаралық экран және ақпараттық жүйелерді қорғау үшін сегрегация сияқты желілік қауіпсіздікті бақылау құралдарын енгізуі тиіс.
2. Жеткізуші құпия және құпия ақпарат санатына жатқызылған дауыстық коммуникацияның қорғалуы мен қауіпсіздігін қамтамасыз етуі тиіс (төменде толық сипатталғандай), яғни шифрлаусыз байланысты пайдалануға тыйым салынған.

5.11 Жүйені сатып алу, әзірлеу және сүйемелдеу (Жеткізуші Kcell үшін бағдарламалық қамтамасыз етуді немесе жүйені әзірлеген кезде)

1. Жеткізуші өзгерту және шолу рәсімдерін қоса алғанда, бағдарламалық қамтамасыз ету мен жүйелерді әзірлеудің бүкіл өмірлік циклі үшін қағидаларды енгізуі тиіс.
2. Жеткізуші бақыланатын ортада әзірлеу процесінде қауіпсіздік функцияларын сынауға міндетті.

5.12 Жеткізушілерге қосалқы мердігерлермен қатынастар

1. Жеткізуші осы Қауіпсіздік жөніндегі директивалардың мазмұнын Келісімге сәйкес міндеттерді орындауға тартылған қосалқы мердігерлермен жасалған шарттарда көрсетуге тиіс.
2. Жеткізуші қосалқы мердігерлердің Қауіпсіздік жөніндегі директиваның талаптарын сақтауын үнемі бақылауға, талдауға және тексеруге міндетті.
3. Жеткізуші Kcell талабы бойынша қосалқы мердігерлердің Қауіпсіздік жөніндегі директиваның талаптарын сақтауына дәлелдемелер беруге міндетті.

5.13 Қауіпсіздік инциденттерін басқару

1. Жеткізушінің Қауіпсіздік инциденттерін басқару бойынша қолданыстағы рәсімдері болуы тиіс.
2. Жеткізуші Kcell-ге қауіпсіздіктің бұзылуына байланысты оқиғалар туралы негізсіз кідіріссіз уақтылы және дәл хабарлауға міндетті.
3. Жеткізуші сот сараптамасын жүргізу кезінде Kcell-ге жәрдемдесуі тиіс.

5.14 Бизнестің үздіксіздігін басқару

1. Жеткізуші бизнестің үздіксіздігіне байланысты тәуекелдерді анықтауы және осындай тәуекелдерді бақылау және төмендету үшін қажетті шараларды қабылдауы тиіс.
2. Жеткізушінің бизнестің үздіксіздігін қамтамасыз ету үшін құжатпен ресімделген процестері мен рәсімдері болуы тиіс.
3. Жеткізуші бизнестің үздіксіздігін басқару тиімділігін бағалауды және қолжетімділік бойынша талаптарды сақтауды (ондай болған жағдайда) кезең-кезеңмен жүргізуге тиіс.
4. Жеткізуші қызмет көрсетуді қамтамасыз ету жөніндегі шараларды, олар болған жағдайда, үнемі тексеріп отыруы тиіс.

5.15 Талаптарды сақтау

1. Жеткізуші Дербес деректерді қорғауды қоса алғанда, бірақ онымен шектелмей, барлық тиісті заңнамалық актілер мен шарттық талаптарды сақтауға тиіс.
2. Жеткізуші сұраным бойынша Kcell-ге осы Қауіпсіздік жөніндегі директиваларда белгіленген талаптардың сақталуы туралы есепті негізсіз кідіріссіз ұсынуы тиіс.
3. Kcell Жеткізушінің және оның қосалқы мердігерлерін Қауіпсіздік жөніндегі директиваны немесе өзге де тиісті талаптарды орындау мәніне тексеруге құқылы.

6 IT ҚАУІПСІЗДІГІ

6.1. Жеткізуші ресурстарына қойылатын талаптар

1. Kcell ақпаратын өңдеу үшін пайдаланылатын Жеткізуші жабдығы және/немесе бағдарламалық қамтамасыз етуі заңнамада, ережелерде және озық салалық практикаларда көзделгендей ақпаратты рұқсатсыз қол жеткізуден тиісті қолданыстағы қорғауы болуы тиіс (мысалы, зиянды бағдарламадан қорғау үшін қауіпсіздікті басқару бағдарламалары, бағдарламалық кіріспелерді басқару, пайдаланушыларды сәйкестендіру, қол жеткізуді бақылау, ақпаратты ашудан қорғау, авариялық жағдайларды анықтау және тіркеу, тіркеу журналдарын басқару, төтенше жағдайлар кезінде жұмыс істеуді қамтамасыз ету, кілттерді басқару, желі қауіпсіздігін басқару және IT-ресурстарды физикалық қорғау).
2. Оларды өңдеу кезінде деректерге зиян келтіретін немесе жүйенің жұмысы үшін зиянды болып табылатын сервистер немесе бағдарламалық қамтамасыз ету шартта айқындалған міндеттерді орындау үшін пайдаланылатын жүйелерде орнатылмауы немесе жандандырылмауы тиіс.
3. Деректерді сақтау және өңдеу жүйелері бағдарламалық қамтамасыз етуді жеткізушінің ұсынымдарына және озық практикаларға сәйкес әзірленуі және күшейтілуі тиіс.
4. Жеткізушінің қызмет көрсету кезінде пайдаланылатын өндірістік жабдықтың үздіксіз жұмыс істеуін қамтамасыз ету жоспары болуы тиіс.
5. Жеткізуші шартта көрсетілген функцияларды жүзеге асыру үшін пайдаланылатын Жеткізушінің меншікті ресурстары ақпараттық қауіпсіздікті бұзу оқиғалары анықталатындай және нақты тұлғаға жатқызылатындай бақыланатындығына кепілдік беруге тиіс. Kcell мен Жеткізуші арасындағы келісім бойынша мониторинг деректері Kcell арқылы беріледі.
6. Жеткізуші оның Kcell атынан өңдейтін ақпаратының резервтік көшірмесін және Жеткізушінің ортасында ақпаратты өңдеу кезінде осындай резервтік көшірмелерді қалпына келтіру мүмкіндігін қамтамасыз етуге міндетті.
7. Резервтік көшірмелер бастапқы деректерді өңдеу кезіндегідей құпиялылықты сақтаудың ұқсас талаптарын сақтай отырып өңделуі тиіс. Резервтік көшірмелер төтенше жағдай туындаған кезде бастапқы деректердің де, сондай-ақ резервтік көшірмелердің де бір мезгілде жойылуын болдырмау үшін бастапқы деректерден бөлек сақталуы тиіс.
8. Жеткізуші оқиғаларды тіркеу журналдарын заңнамаға сәйкес немесе шартта айқындалғандай өзгеше түрде сақтауға міндетті. Kcell ақпараттық қауіпсіздік инциденттерін қарау және реттеу кезінде Kcell-ге қатысы бар оқиғаларды тіркеудің тиісті журналдарына дереу қол жеткізуі тиіс.
9. Жүйелік әкімшілер және басқа да жоғары артықшылықты пайдаланушылар аутентификацияны қатаң (2 факторлық) аутентификацияны пайдалана отырып жүзеге асыруға тиіс.
10. Қашықтықтан қол жеткізу мүмкіндігі бар пайдаланушылар сенімсіз желілерден жүйеге қол жеткізген кездерінде қатаң аутентификацияны пайдалана отырып орнатылады.
11. Ноутбуктер мен тасымалданатын тасымалдағыштар Жеткізушінің үй-жайларынан тыс жерлерге пайдалану немесе жылжыту кезінде шифрлауға жатады.

6.2 Kcell ресурстарына қойылатын талаптар

1. Kcell ұсынатын жабдықтар мен АТ-функционалдығы келісілген қызметтерді орындау үшін ғана пайдаланылуы тиіс.
2. Kcell ұсынатын жабдықтар мен IT-функционалдығы Kcell нұсқаулықтарына сәйкес пайдаланылуы тиіс.
3. Жеткізуші кездейсоқ жоғалудан немесе ұрлықтан қорғауға қолдау көрсету кезінде Kcell активтерін қорғауды қамтамасыз етуі тиіс.

6.3 Ақпараттық қауіпсіздік

1. Жеткізуші ол өңдейтін және «Кселл» АҚ-ға тиесілі ақпараттың қауіпсіздігін қамтамасыз етуге тиіс. Жеткізуші «Кселл» АҚ ақпаратын өңдеген кезінде адал және жергілікті заңдарға сәйкес әрекет етуге міндетті.
2. «Кселл» АҚ ұсынған барлық Құпия ақпарат Жеткізуші оны өңдеген кезде мынадай талаптарға сәйкес келуі тиіс:
    - Қағаз тасығыштардағы құжаттар, түсірілім ақпарат тасығыштары және т.б. уәкілетті тұлғаның қатаң бақылауында сақталуы және «Кселл» АҚ Құпиялылық белгісін анықтау жөніндегі нұсқаулыққа сәйкес немесе «Кселл» АҚ ақпараттық қауіпсіздігінің жалпы рәсімдеріне сәйкес өңделуі тиіс.
    - «Кселл» АҚ-ға жататын ақпаратты дауыспен беру қауіпсіздік режимін сақтай отырып жүзеге асырылуы тиіс. Бұл басқалардың арасында сымсыз телефон жүйелерінің баламасы, жалпыға бірдей қолжетімді IP-телефония немесе шифрланбаған радиобайланыс пайдаланылмайды дегенді білдіреді. Қоғамдық үй-жайлардан ақпарат беруге жол берілмейді.
    - «Кселл» АҚ деректерін беру қауіпсіз режимде жүзеге асырылады (мысалы, беру кезінде өтпелі шифрлауды пайдалана отырып, «Кселл» АҚ сенімді байланыс арналарын пайдалана отырып немесе әдетте бағдарламалық

қамтамасыз етуді пайдаланатын қауіпсіздік шараларын пайдалана отырып). Бұл ережеден алып тастау «Кселл» АҚ-ның жазбаша келісімін талап етеді.

- Жеткізуші персоналы ешқандай жағдайда келісілген тапсырманы орындау үшін қажеттілігі жоқ ақпаратқа немесе Жеткізушінің персоналына рұқсат берілмейтін ақпаратқа әдейі қол жеткізуге тырысуға құқылы емес. Егер Жеткізуші Персоналы қатарындағы кез келген қызметкер ақпаратқа әдейі рұқсатсыз қол жеткізетін болса, онда «Кселл» АҚ бұл туралы дереу хабардар етілуі тиіс.

3. Ақпаратты өңдеуге қатысты Жеткізушіне «Кселл» АҚ үшін орындалатын міндеттер шеңберінде деректер файлдарында, баспа тасығыштарда немесе басқа да материалдық жеткізгіштерде сақталатын ақпаратты көшіруге және ойнатуға ғана рұқсат етілген.
4. Жеке пайдалануға арналған көшірмелерді (жұмыс көшірмесін) жүргізетін адам, егер олар бұдан әрі пайдаланылмайтын болса, оларды жоюға жауапты болады.
5. Көшіру немесе ойнату ақпарат иесінің таңбалауын немесе қауіпсіздік санатын жоюға әкеп соқпауы тиіс.
6. Жеткізуші барлық жағдайларда деректер файлдарында, баспа тасығыштарда немесе басқа да материалдық жеткізгіштерде сақталатын ақпаратты, Жеткізушінің үй-жайларында ақпараттың өңделіп жатқанына немесе өңделмегеніне қарамастан, бөгде адамдарға ақпаратқа қол жеткізу үшін айтарлықтай күш-жігер қажет ететіндей етіп өңдеуге тиіс.
7. Жеткізуші ақпаратты Жеткізуші өңдейтіндігіне және шартқа қатысты ақпараттың шартпен байланысты емес ақпаратпен араласпайтындығына кепілдік береді.
8. Өндірісте пайдаланылатын деректер әзірлену немесе тестілеу үшін ешқандай жағдайда пайдаланылмауы тиіс. Сонымен қатар, егер тест деректерін пайдалану мүмкін болмаса, онда жүйе өндіріске қатысты қолданылатын осыған ұқсас қауіпсіздік талаптарына жауап беруі тиіс.
9. Өндіріс саласынан тестілеу мақсатында ақпарат алуға тек «Кселл» АҚ-ның жазбаша келісімімен ғана жол беріледі.
10. Шарт тоқтатылған кезде немесе егер тапсырманы орындау енді деректерді өңдеуді талап етпесе, Жеткізуші «Кселл» АҚ атынан орындалатын өңдеуге байланысты барлық деректерді «Кселл» АҚ-ға беруге немесе мүмкіндігінше оны жою куәлігін беруге міндетті.

7 Құпиялылық санаттарының сипаттамасы және құпия ақпаратпен жұмыс істеу қағидалары

Санат	Сипаттамасы	Ақпарат түрлерінің мысалдары
Құпия	Рұқсатсыз қол жеткізу немесе ақпаратты ашу Kcell-ге, оның ұйымына, маңызды функцияларға, жұмыс күшіне, іскерлік әріптестерге және/немесе клиенттерге **елеулі зиян** келтіруі мүмкін.	- жылдық есеп және қызмет нәтижелері ресми жарияланғанға дейін - құқықтық сипаттағы белгілі бір ақпарат, клиенттермен жасалған кейбір шарттар немесе құпия ақпаратты жария етпеу туралы келісімдер.
Құпия	Рұқсатсыз қол жеткізу немесе ақпаратты ашу Kcell-ге, оның ұйымына, маңызды функцияларға, жұмыс күшіне, іскерлік әріптестерге және/немесе клиенттерге **зиян** келтіруі мүмкін.	- құқықтық сипаттағы белгілі бір ақпарат, мысалы, клиенттердің немесе қызметкерлердің жеке деректері - құпия бизнес-жоспарлар, стратегиялар мен шешімдер (мысалы, маркетингтік жоспарлар)
Ішкі	Рұқсатсыз қол жеткізу немесе ақпаратты ашу Kcell-ге, оның ұйымына, маңызды функцияларға, жұмыс күшіне, іскерлік әріптестерге және/немесе клиенттерге **шамалы зиян** келтіруі мүмкін.	- Kcell ішкі пайдалануға арналған ақпарат - Kcell қызметкерлеріне арналған, мысалы, ұйыммен, стратегиямен, өніммен, қызметкерлерге қызмет көрсетумен байланысты ақпараттық материалдар
Жария	Рұқсатсыз қол жеткізу немесе ақпаратты ашу Kcell-ге, оның ұйымына, маңызды функцияларға, жұмыс күшіне, іскерлік әріптестерге және/немесе клиенттерге **еш зиян** келтірмейді.	- жылдық есеп және қызмет нәтижелері ресми жарияланғаннан кейін - жарияланған маркетингтік материалдар мен баспасөз релиздері - заң талаптарына сәйкес жария етілетін ақпарат

Санат	Ақпаратқа кім қол жеткізе алады	Қалай сақтау керек	Қалай жіберу керек	Қалай пайдалану керек	Қорғау қажеттілігін қалай бағалауға болады (тәуекелдерге негізделген тәсіл)

Құпия	Тек тағайындалған адамдар	Логикалық және физикалық қауіпсіз сақтау, яғни қол жеткізуді шифрлау немесе бұғаттау	Қорғалған байланыс арналары бойынша немесе қорғалған портативті жинақтауышта (бұғатталған түрде)	Кіру және тыңдаудан қорғалған қауіпсіз салаларда пайдалану үшін (бөгде адамдар)	Қорғаныс бұзуға төзімді болуы тиіс. Тек қатты мүдделі және/немесе өнертапқыш қаскүнемдер қорғанысты бұза алады.
Құпия	Тек шектеулі және бақыланатын тұлғалар тобы	Қол жеткізуді қатаң бақылау кезінде логикалық және физикалық бақыланатын сақтау *	Қорғалған байланыс арналары бойынша немесе бақыланатын және сенімді желі бойынша немесе қорғалған портативті жинақтауышта*	Уәкілетті адамдардың коммерциялық мақсаттарда тек бақыланатын жұмыс кеңістігі немесе кіру мен тыңдаудан қорғалған орын шегінде (бөгде адамдар) пайдалануы үшін	Бөгде адамдардың ақпаратқа қол жеткізуі қиын. Тек мүдделі қаскүнемдер ғана қорғанысты бұза алады.
Ішкі	Kcell АҚ үшін жұмыс атқаратындар	Қол жеткізуді логикалық және физикалық бақылау	Қорғалған байланыс арналары бойынша немесе бақыланатын және сенімді желі бойынша	Уәкілетті адамдардың коммерциялық мақсаттарда тек бақыланатын жұмыс кеңістігі немесе кіру мен тыңдаудан қорғалған орын шегінде (бөгде адамдар) пайдалануы үшін	Бөгде адамдардың ақпаратқа қол жеткізу мүмкіндігі шамалы. Тек мүдделі қаскүнемдер ғана қорғанысты бұза алады.
Жария	Шектеусіз	Шектеусіз	Шектеусіз	Шектеусіз	Шектеусіз