АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Астана
2023 жыл

Жалпы ереже

Осы Qazaq Green certificate Registry ақпараттық жүйесінің ақпараттық қауіпсіздік саясаты (бұдан әрі – саясат) ақпарат қауіпсіздігін қамтамасыз ету қағидаттарының жүйесін айқындайды және Qazaq Green Certificate Registry операторы – «Qazaq Green» ЖЭК қауымдастығында (бұдан әрі – ұйым) ақпараттың қауіпсіздігін қамтамасыз етудің қорғау мақсаттары мен міндеттерін, құрылыстың негізгі қағидаттарын, ұйымдастырушылық, технологиялық және рәсімдік аспектілерін жүйелі түрде баяндауды білдіреді.

Саясат ұйымдағы ақпараттық технологияларды дамытудың қазіргі жағдайы мен таяудағы перспективаларын, оларды пайдаланудың мақсаттарын, міндеттері мен құқықтық негіздерін, жұмыс істеу режимдерін ескереді, сондай-ақ ұйымның ақпараттық қатынастарының объектілері мен субъектілері үшін қауіпсіздікке төнетін қатерлердің тізбесін қамтиды.

Осы саясаттың талаптары ұйымның барлық құрылымдық бөлімшелеріне қолданылады.

Саясат «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасының заңына, Қазақстан Республикасының нормативтік құқықтық актілеріне, сондай-ақ Қазақстан Республикасының басқа да нормативтік құқықтық актілеріне сәйкес әзірленді.

Саясат үшін әдіснамалық негіз:

1) ұйымдағы ақпараттың қауіпсіздігін қамтамасыз ету саласында бірыңғай саясатты қалыптастыру және жүргізу;

2) қорғауға жататын ақпаратты анықтау, оның құпиялылық деңгейін негіздеу және тиісті тізбелер түрінде құжаттамалық ресімдеу жөніндегі жұмыстарды ұйымдастыру;

3) басқару шешімдерін қабылдау және ақпарат қауіпсіздігі саясатын іске асыру бойынша практикалық шараларды әзірлеу;

4) ақпарат қауіпсіздігіне төнетін түрлі қатерлерді іске асыру салдарын анықтауға, көрсетуге және жоюға бағытталған келісілген шаралар кешенін әзірлеу;

5) ақпараттың қауіпсіздігін қамтамасыз ету жөніндегі талаптарды сақтай отырып, ақпараттық технологияларды құру, дамыту және пайдалану жөніндегі жұмыстарды жүргізу кезінде ұйымның құрылымдық бөлімшелерінің қызметін үйлестіру;

6) ұйымдағы ақпарат қауіпсіздігін құқықтық, нормативтік, техникалық және ұйымдастырушылық қамтамасыз етуді жетілдіру бойынша ұсыныстар әзірлеу болып табылады.

Ақпараттық ресурстарды қорғау мыналарға сәйкес келетін ақпараттық қауіпсіздікті басқару жүйесі шеңберінде жүзеге асырылады:

- ҚР СТ ИСО/МЭК 27001-2015 ақпараттық қауіпсіздік стандарты талаптары.

- ақпараттық қауіпсіздік тұрғысынан Қазақстан Республикасы заңнамасының талаптары, ұйымның нормативтік және шарттық міндеттемелері;

- ұйымның осы ақпараттық қауіпсіздік саясаты.

Ұйымның ақпараттық қауіпсіздігін басқару жүйесінің қолданылу саласы: ұйымның ақпараттық жүйелерінің үздіксіз жұмыс істеуіне қатысты ақпараттық қауіпсіздікті басқару болып табылады.

Ұйым басшылығы ұйымдағы ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызмет үшін жауапкершілікті толығымен өзіне алады, жоғарыда аталған мақсаттар мен қағидаттарға өзінің адалдығын мәлімдейді, сондай-ақ ұйымның барлық қызметкерлер құрамын осыған міндеттейді. Ұйым қызметкерлері АҚБЖ құжаттарының талаптарын сақтауға дербес жауапты болады және ақпараттық қауіпсіздік саласында анықталған барлық бұзушылықтар туралы хабарлауға міндетті.

Ақпараттық қауіпсіздікті басқару жүйесін құрудың осы саясаты жылына кемінде бір рет тұрақты түрде қайта қаралуы тиіс.

Саясат келесі негізгі мақсаттарға жетуге бағытталған:

1) ұйымда пайдаланылатын және өңделетін ақпараттың тұтастығын қорғау;

2) маңызды ақпараттық ресурстардың құпиялылығын сақтау;

3) тіркелген пайдаланушылар үшін өңделетін ақпараттың қолжетімділігін қамтамасыз ету;

4) ұйымда жұмыс істейтін негізгі бизнес-процестердің үздіксіздігін қамтамасыз ету.

Көрсетілген мақсаттарға қол жеткізу үшін мынадай міндеттерді шешу қажет:

1) кәсіпорынның ақпараттық қауіпсіздігін басқаруға басшылықтың белсенді қатысуы;

2) қызметкерлердің ақпараттық ресурстармен байланысты тәуекелдер туралы хабардарлығын арттыру;

3) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметкерлердің жауапкершілігі мен міндеттерін нақты бөлу;

4) тіркелген пайдаланушылардың кәсіпорынның аппараттық, бағдарламалық және ақпараттық ресурстарына қол жеткізуін шектеу;

5) желілік ресурстарды пайдалану кезінде жүйелік журналдарда пайдаланушылардың әрекеттерін тіркеу;

6) осы журналдардың мазмұнын талдау арқылы жүйелерді пайдаланушылардың әрекеттерінің дұрыстығын бақылау;

7) ақпараттық жүйелердің жұмыс істеу процесіне бөгде адамдардың араласуынан қорғау;

8) пайдаланылатын бағдарламалық құралдардың тұтастығын, бағдарламалардың орындалу ортасын бақылау және бұзылған жағдайда оны қалпына келтіру, сондай-ақ жүйелерді зиянды кодтарды енгізуден қорғау;

9) таралуы шектеулі ақпаратты, дербес деректерді оны өңдеу, сақтау және байланыс арналары арқылы беру кезінде техникалық арналар бойынша таралудан қорғау;

10) ақпараттық жүйелер мен ресурстарды пайдаланушылардың аутентификациясын қамтамасыз ету;

11) ақпараттық қауіпсіздікке төнетін қатерлерді, зиян келтіруге ықпал ететін себептер мен жағдайларды уақтылы анықтау;

12) жеке және заңды тұлғалардың заңсыз әрекеттерімен келтірілген залалды азайту және оқшаулау үшін жағдайлар жасау;

13) ақпараттық қауіпсіздік саясаты бұзылған жағдайда тәртіптік жаза практикасын жүргізу;

14) ақпараттық қауіпсіздікті бұзу салдарын жою;

15) кәсіпорын қызметкерлерінің ақпараттық қауіпсіздікті қамтамасыз ету, тиісті талаптардың орындалуын бақылау жөніндегі қағидалар мен нұсқаулықтарды әзірлеу және енгізу;

16) ақпараттық тәуекелдерді бағалау және басқару жөніндегі іс-шараларды іске асыру;

17) ақпараттық қауіпсіздікті басқару жүйесін жетілдіру.

1. Басшылықтың жауапкершілігі мен міндеттемелері

Тиімді қауіпсіздік есеп беруді, қауіпсіздік міндеттерін толық анықтауды және мойындауды талап етеді. Басшылық қауіпсіздікті басқарудың барлық аспектілеріне, соның ішінде тәуекелдерді басқару шешімдерін қабылдауға жауапты болуы керек. Ұйымның түрі, тіркеу нысаны, мөлшері және құрылымы сияқты оның жеке факторлары осы міндеттердің қай деңгейде анықталатынына әсер етеді. Ақпараттық қауіпсіздік – бұл кәсіпорын ішіндегі барлық пайдаланушыларға қатысты пәнаралық тақырып. Есептілікті, нақты қызметтік міндеттер мен жауапкершілікті дұрыс анықтау және саралау барлық маңызды міндеттердің тиімді және білікті орындалуын қамтамасыз етуі керек.

Басшылық ұйым (бизнес) қызметінің мақсаттарына, заңдар мен нормативтік актілерге сәйкес ақпараттық қауіпсіздікті қамтамасыз етуге байланысты мәселелерді шешуге тікелей қатысады.

Басшылық менеджмент жүйесін енгізу жолымен, сондай-ақ оны қамтамасыз ету үшін қызметкерлердің міндеттері мен жауапкершілігін бөлу жолымен (жауапты тұлғаларды тағайындау туралы бұйрық, лауазымдық нұсқаулықтар және т.б.) ақпараттық қауіпсіздіктің берілген деңгейін қолдауды жүзеге асырады.

Басшылық:

1. ақпараттық қауіпсіздік саясатын тұжырымдау, қайта қарау және бекіту, сондай-ақ ақпараттық қауіпсіздік саясатын іске асырудың тиімділігін бақылау;
2. ақпараттық қауіпсіздік саласындағы бастамаларды нақты басқаруды және нақты қолдауды қамтамасыз ету;
3. ақпараттық қауіпсіздікті қамтамасыз ету үшін ресурстармен қамтамасыз ету;
4. ұйымдағы ақпараттық қауіпсіздікті бақылау шараларын үйлестіруді қамтамасыз ету;
5. лауазымдық нұсқаулықтар, бұйрықтар, жарлықтар және т.б. арқылы ұйымдағы ақпараттық қауіпсіздік жөніндегі қызметкерлердің рөлдері мен міндеттерін бекіту;
6. ақпараттық қауіпсіздік туралы хабардарлықты сақтау идеяларына, жоспарлары мен бағдарламаларына бастама жасау, пайдаланушылар мен әкімшілерді қауіпсіздік әдістері мен рәсімдеріне үйрету қажеттілігін анықтау, бағдарламалық қамтамасыз ету мен аппараттық құралдарды орнатуға және қызмет көрсетуге қатысты міндеттерді анықтау;
7. ұйым ішінде немесе тараптан ақпараттық қауіпсіздік мәселелері бойынша маманмен кеңесу қажеттілігін анықтау, ұйым бойынша консультация нәтижелерін қарау және үйлестіру;
8. әр түрлі активтер мен қауіпсіздік процестері үшін бөлім басшыларының жауапкершілігін нақты анықтау, осы жауапкершіліктің егжей-тегжейлері құжатталуы тиіс, өкілеттік деңгейлері нақты анықталуы және құжатталуы керек (материалдық жауапкершілік туралы акт);
9. ақпараттық қауіпсіздік саясаты бұзылған жағдайда тәртіптік жаза практикасын жүргізу;
10. ақпараттық қауіпсіздікті бұзу салдарын жою.

Қызметкерлер өздерінің функционалдық міндеттеріне сәйкес ақпаратты жария еткені үшін жауапкершілік шараларымен, сондай-ақ ықтимал бұзушылықтар үшін жауапкершілік шараларымен танысуы тиіс.

АЖ қызмет көрсетуші персоналы АҚ саясаты тармақтарының талаптары бұзылған кезде Қазақстан Республикасының қолданыстағы заңнамасына сәйкес әкімшілік немесе өзге де жауаптылыққа тартылады. АЖ әкімшілеріне жауапкершілік сервер әкімшісінің функциялары мен өкілеттіктерін бекіту жөніндегі нұсқаулыққа сәйкес олардың жауапкершілігіне сәйкес жүктеледі. Атап айтқанда, АЖ ресурстарының әкімшілері желінің үздіксіз жұмыс істеуін қамтамасыз етеді және қауіпсіздік саясатын жүзеге асыру үшін қажетті техникалық шараларды іске асыруға жауап береді.

3. Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі қағидаттары

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі қағидаттары:

1) Қазақстан Республикасы заңнамасының талаптарын сақтау;

2) Қазақстан Республикасының аумағында қолданылатын ақпараттық қауіпсіздік саласындағы халықаралық және ұлттық стандарттарға сәйкестігі;

3) ақпараттық активтердің осалдығын анықтау мақсатында ақпараттық кеңістікті тұрақты және жан жақты талдау;

4) ықтимал проблемалардың себеп-салдарлық байланыстарын анықтау және осы негізде олардың дамуының нақты болжамын құру;

5) анықталған проблемалардың әсер ету дәрежесін ақылға қонымды бағалау;

6) қауіптерді іске асырудың барлық маңызды арналарын жабатын және оның жекелеген компоненттерінің түйіскен жерінде әлсіз жерлері жоқ компьютерлік жүйелерді қорғау әдістері мен құралдарын кешенді пайдалану. Қорғау физикалық құралдармен, ұйымдастырушылық, технологиялық және құқықтық шаралармен қамтамасыз етілуі керек. Бұл ретте ақпараттық қауіпсіздікті қамтамасыз ету үшін қабылданатын шаралар жарғылық мақсаттарға қол жеткізуді қиындатпауға, сондай-ақ ақпаратты өңдеудің технологиялық процестерінің күрделілігін арттыруға тиіс;

7) қабылданған қорғау шараларын тиімді іске асыру;

8) уақыт өте келе сыртқы жағдайлар мен талаптардың ықтимал өзгеруіне байланысты қауіпсіздік деңгейінің өзгеруін қамтамасыз ету үшін қорғаныс құралдарының икемділігі;

9) ұйымдастырушылық және техникалық шешімдердің сабақтастығы негізінде ақпаратты қорғау шаралары мен құралдарын жетілдіру, ақпаратты ұстау әдістері мен құралдарындағы өзгерістерді және олардың компоненттеріне әсер етуді, қорғау жөніндегі нормативтік талаптарды, осы салада қол жеткізілген отандық және шетелдік басқа

ұйымдардың тәжірибесін ескере отырып, ақпараттық жүйелердің жұмыс істеуін талдау;

10) қауіпсіз жұмыс істеу қағидаттарының үздіксіздігі.

11) ақпараттық қауіпсіздікті қамтамасыз етудің белгіленген қағидаларын бұзу әрекеттерін анықтаудың міндеттілігі мен уақтылығы, жолын кесу. Пайдаланушылардың қызметін, әрбір құралды және кез келген қорғау объектісіне қатысты бақылау жедел бақылау және тіркеу құралдарын қолдану негізінде жүзеге асырылуы тиіс және пайдаланушылардың рұқсатсыз да, санкцияланған да әрекеттерін қамтуы тиіс;

12) ұйымдық құрылымдағы белгісіздікті, қызметкерлердің рөлін, бекітілген саясатты және қабылданған қорғау шараларының барабарлығын бағалау мүмкін невозможстігін болдырмау үшін құжаттардағы ақпараттық қауіпсіздіктің функционалдық мақсаттары мен мақсаттарын нақты айқындау;

13) ақпараттың қауіпсіздігін және оның өкілеттігі шегінде әрбір қызметкер үшін оны өңдеу жүйесін қамтамасыз ету үшін дербес жауапкершілікті айқындау. Осы қағидатқа сәйкес қызметкерлердің құқықтары мен міндеттерін бөлу кез келген бұзушылық болған жағдайда кінәлілер шеңбері нақты белгілі немесе минимумға дейін болатындай етіп құрылуы керек;

14) тиісті шарттарда (келісімдерде) және/немесе өзге де құжаттарда айқындалған белгіленген мерзімдерде өз клиенттері мен контрагенттері үшін қызметтер мен сервистердің қолжетімділігін қамтамасыз ету;

15) ақпараттық қауіпсіздікті қамтамасыз етуді байқау және бағалау мүмкіндігі, қорғау шараларын қолдану нәтижесі анық байқалуы (ашық) және тиісті өкілеттіктері бар маман бағалауы мүмкін;

16) өңделетін ақпаратты жіктеу, Қазақстан Республикасының заңнамасына сәйкес оның маңыздылық деңгейін айқындау.

4. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі кадр саясаты

Қызметкерлердің функциялары мен міндеттері лауазымдық нұсқаулықта нақты анықталған және жұмысқа қабылдау кезінде кандидаттарға хабарланған.

Қызметкерлер өздерінің жауапкершілігі мен кәсіпорынның ақпараттық қауіпсіздікке қатысты жауапкершілігі белгіленген еңбек шартының талаптарына қол қояды.

Ұйымның ақпаратты өңдеу құралдарын пайдаланатын үшінші тарап ұйымдарының қызметкерлері мен өкілдері ұрлықтан, алаяқтықтан және жабдықты мақсатсыз пайдаланудан, сондай-ақ ақпарат қауіпсіздігіне төнетін

қатерлерден болатын тәуекелдерді азайту мақсатында ақпараттық қауіпсіздік талаптарына сәйкес келісімге қол қоюы тиіс.

Құпиялылықты сақтау және жарияламау туралы келісімге қызметкер, мердігер немесе пайдаланушы ақпаратты өңдеу құралдарына қол жеткізгенге дейін үшінші тарап ұйымы қол қояды.

Тұрақты жұмысқа барлық кандидаттарды тексеру ҚР қолданыстағы еңбек заңнамасына сәйкес жеке деректердің құпиялылығын сақтай отырып жүргізілуі тиіс. Кандидат беретін мынадай ақпарат тексеруге жатады:

1) алдыңғы жұмыс орындарынан ұсынымдар;
2) үміткердің түйіндемесі;
3) білім және кәсіптік біліктілік туралы құжаттар;
4) жеке басын куәландыратын құжаттар;
5) нақтылауды қажет ететін басқа ақпарат.

Тұрақты штатқа қабылданатын барлық қызметкерлер туралы ақпарат ҚР қолданыстағы еңбек заңнамасына сәйкес жиналуы және өңделуі тиіс.

Қызметкерлер осы саясаттың талаптарымен, ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қағидалармен және нұсқаулықтармен, танысу парағына міндетті түрде қол қоя отырып, оқыс оқиғаларға ден қою және олардың алдын алу рәсімдері туралы хабардар ету мақсатында танысуы тиіс.

Қызметкерлердің еңбек шартының қолданысы аяқталғаннан кейін пайдалануындағы барлық активтердің (есептеу техникасының құралдары, қызметтік құжаттар, электрондық жеткізгіштер және т.б.) қайтарылуын бақылауды жүзеге асыру, сондай-ақ қызметкер жеке жабдықты пайдаланған жағдайда, ақпаратты тиісті бөлімшенің басшысына (жауапты маманға) беруді немесе жабдықтан қалпына келтірілмейтін әдістермен ақпаратты жоюды қамтамасыз ету қажет.

Ақпараттық жүйелер мен ресурстарға қол жеткізу құқығы қызметкердің еңбек шартының (жұмыстан босатылуының) қолданысы аяқталғаннан кейін жойылады немесе оның міндеттері мен функциялары өзгерген кезде қайта қаралуға жатады.

Белсенді болып қалған есептік жазбалар үшін құпия сөздер ұзақ іссапарға, демалысқа немесе еңбек шартының қолданылуының аяқталуына байланысты туындаған еңбек қызметі тоқтатылған кезде өзгертілуі тиіс.

5. Ақпараттық қауіпсіздік саясатын қайта қарау

Кәсіпорынның ақпараттық қауіпсіздік саясатының ережелері жоспарға сәйкес жылына кемінде бір рет жүйелі түрде қайта қарауды және түзетуді талап етеді.

Қауіпсіздік саясатын жоспардан тыс қайта қарау мына жағдайларда

жүргізіледі:

1) АЖ-ға маңызды өзгерістер енгізу;
2) заңнамадағы, ұйымдық құрылымдағы өзгерістер;
3) ақпараттық қауіпсіздік инциденттерінің пайда болуы.

Өзгерістер енгізу кезінде мыналар ескеріледі:

1) ақпараттық қауіпсіздік аудитінің нәтижелері, сондай-ақ алдыңғы аудиттердің нәтижелері;
2) ақпараттық қауіпсіздік бойынша тәуелсіз сарапшылардың ұсыныстары;
3) ақпараттық жүйенің елеулі қауіптері мен осалдықтары;
4) ақпараттық қауіпсіздік саласындағы оқиғалар туралы есептер;
5) мемлекеттік органдардың ұсынымдары.

Саясатты қайта қарауды оны әзірлеуге, енгізуге жауапты мамандар жүзеге асырады және оның ережелерін жақсарту мүмкіндігін және өзгерістерге сәйкес ақпараттық қауіпсіздікті басқару процесін бағалауды қамтиды.

Ақпараттық қауіпсіздік саясатын қайта қарау ҚР СТ ИСО/МЭК 27002-2009 іске асыру жөніндегі нұсқаулыққа сәйкес жүзеге асырылуы тиіс.

Осы саясат АЖ үшін ақпараттық қауіпсіздік тәуекелдеріне талдау жүргізу және бағалау нәтижелері бойынша міндетті түрде қайта қаралуы және қажеттігіне қарай өзектендірілуі тиіс.

Ақпараттық қауіпсіздіктің қайта қаралған саясатын уәкілетті адамдар бекітеді.

ТАНЫСУ ПАРАҒЫ

№	Тегі, аты, әкесінің аты	Лауазымы	Жеке қолы	Күні
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				