

"Транстелеком" АҚ Ақпараттық қауіпсіздік саясаты

1. Жалпы ережелер

1.1. Осы Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) ақпараттық қауіпсіздік саласындағы негізгі құжат болып табылады және «Транстелеком» АҚ-да (бұдан әрі – Қоғам) тиісті ішкі нормативтік құжаттарын әзірлеу кезінде нұсқаулық болып табылады.

1.2. Саясат қоғамның бизнес стратегиясы мен бизнес мақсаттарын іске асыру мақсатында әзірленеді.

1.3. Ақпараттық қауіпсіздік шеңберінде Қоғам өз мүдделерін (мақсаттарын) ақпараттық саладағы қауіптерден қорғау жағдайын түсінеді. Қауіпсіздікке Қоғамның ақпараттық активтерінің қасиеттерінің жиынтығын қамтамасыз ету арқылы қол жеткізіледі: құпиялылық, тұтастық және қолжетімділік.

1.4. Қоғамда ақпараттық-коммуникациялық инфрақұрылымның қауіпсіздігін қамтамасыз ету мақсатында байланыс, автоматтандыру, энергетика, ақпараттық технологиялар және ақпараттық қауіпсіздік саласында қызметтер мен шешімдерді ұсыну кезінде Ақпараттық қауіпсіздікті басқару жүйесі (бұдан әрі – АҚБЖ) пайдаланылады. АҚБЖ Қоғамның барлық құрылымдық бөлімшелеріне, оның ішінде Қоғамның филиалдарына қолданылады.

1.5. Қоғам ақпараттық қауіпсіздік менеджментінің стандартына сәйкес ҚР СТ ISO/IEC 27001-2015 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздік менеджментінің жүйелері. Талаптар», сондай-ақ ақпараттық қауіпсіздікке қатысты Қазақстан Республикасы заңнамасының, стандарттарының және нормативтік талаптарына сәйкес АҚБЖ жұмыс қалпында ұстау және дамыту есебінен ақпараттық қауіпсіздікті қамтамасыз етудің халықаралық талаптарына сәйкес болуға тырасады.

1.6. Қоғамның АҚБЖ қамтамасыз ету Қоғамда корпоративтік менеджмент қағидаттары мен моделіне сәйкес келетін ақпараттық қауіпсіздік менеджментінің циклдік моделі (Деминг циклі «PDCA – Plan-Do-Check-Act») шеңберінде ұсынылады: «жоспарлау – іске асыру – тексеру – жетілдіру».

1.7. Саясаттың ережелері Қоғамның ақпараттық-коммуникациялық инфрақұрылымына қолжетімділігі бар Қоғамның барлық қызметкерлеріне қолданылады, сонымен қатар контрагенттермен (өнімді тұтынушылар, жеткізушілер, серіктестер, кеңесшілер, тағылымдамадан өтушілер, тәжірибеленушілер т.б.).

1.8. Саясат барлық мүдделі тараптар үшін шектеусіз қолжетімді болуы мүмкін жалпыға ортақ құжат болып табылады.

2.1. Қоғамның ақпараттық қауіпсіздік саласындағы мақсаттары Қоғамның АҚБЖ негізгі мақсаты Қоғамның тұрақты жұмыс істеуін және ақпараттық қауіпсіздік саласындағы қауіптердің алдын алу және тәуекелдер деңгейін барынша азайту арқылы пайдаланылатын ақпараттық-коммуникациялық инфрақұрылымның сенімділігін қамтамасыз ету болып табылады.

2.1.2. Қойылған мақсатқа жету Қоғамның келесі міндеттерді орындауымен қамтамасыз етіледі:

- бизнес-процестердің жоғары сапасын қолдау мақсатында Қоғамның ақпараттық-коммуникациялық инфрақұрылымының тұтастығын, үздіксіздігін және қолжетімділігін қамтамасыз ету;

- ақпараттық қауіпсіздікті қамтамасыз ету бойынша нормативтік-құқықтық ұйымдастырушылық-әкімшілік және материалдық-техникалық шараларын жүзеге асыру;

- ақпараттық қауіпсіздік саласындағы қызметкерлердің кәсіби біліктілігін арттыру;

- Қоғамның ақпараттық қауіпсіздік саласындағы заманауи қауіптер мен тәуекелдерге

тиімді ден қою;

- ақпараттық қауіпсіздік бөлігінде заң талаптары мен шарттық міндеттемелерді сақтау;
- ақпараттық қауіпсіздікті сақтау процесін жүзеге асыруға барлық қызметкерлерді тарту.

2.2.1. Қойылған мақсаттарға қол жеткізу үшін Қоғам келесі принциптерді басшылыққа алуды көздейді:

1) **Ақпараттық қауіпсіздікті қамтамасыз ету процесіне Қоғамның басшылығын тарту** – ақпараттық қауіпсіздік бойынша қызметтер Қоғамның басшылығының (Басқарма Төрағасы, Басқарма төрағасының орынбасарлары) бастамасымен және бақылауымен жүзеге асырылады. Қоғамның басшылығы Қоғамның барлық қызметкерлері сияқты ақпараттық қауіпсіздік бойынша ережелерді сақтайды;

2) **Ақпараттық қауіпсіздікті қамтамасыз етудің заңдылығы** – ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған іс-әрекеттер қолданыстағы заңнамаға және шарттық міндеттемелерге қатаң сәйкестендірілген;

3) **Экономикалық мақсаттылық** – Қоғам ақпараттық қауіпсіздікті қамтамасыз ету бойынша шараларды, оларды іске асыру шығындарын, ақпараттық қауіпсіздік қатерлерінің туындау ықтималдығын және оларды іске асырудан болатын ықтимал шығындар көлемін ескере отырып таңдауға ұмтылады;

4) **Өз қызметкерлерін білу** – Қоғам персоналдарды (қызметкерлерді) мұқият іріктеуге, корпоративтік этиканы дамытуға және сақтауға ұмтылады, бұл Қоғамның қызметі үшін қолайлы жағдай жасайды және ақпараттық қауіпсіздік тәуекелдерін азайтады;

5) **Ақпараттық қауіпсіздік талаптарын құжаттау** – Қоғам ақпараттық қауіпсіздік саласындағы барлық талаптар Қоғам басшылығы бекіткен ішкі нормативтік құжаттарда жазылуын қамтамасыз етуге ұмтылады;

6) **Ақпараттық қауіпсіздікті білу** – ақпараттық қауіпсіздік саласындағы құжатталған талаптар Қоғам қызметкерлерінің және оларға қатысты бөлігінде контрагенттердің назарына жеткізіледі. Қоғам қызметкерлерді ақпараттық қауіпсіздік мәселелері бойынша мерзімді түрде хабардар етеді және оқытады;

7) **Ақпараттық қауіпсіздік инциденттеріне ден қою** – Қоғам ақпараттық қауіпсіздіктің нақты, ағымдағы және ықтимал бұзушылықтарын анықтауға, есепке алуға және оларға жедел ден қоюға ұмтылады;

8) **Жеке жауапкершілік** - Компания қызметкерлері (барлық деңгейде) ақпараттық қауіпсіздік талаптарының сақталуына дербес жауапты болады. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі міндеттер еңбек шарттарында және қызметкерлердің лауазымдық нұсқаулықтарында, сондай-ақ мердігерлермен жасалған шарттарда (келісімдерде) қамтылады;

9) **Ақпараттық активтермен әрекеттерді есепке алу** – Қоғам өзінің ақпараттық активтерінде Қоғам қызметкерлерінің және контрагенттерінің барлық әрекеттерінің есебін жүргізуге ұмтылады;

10) **Ең аз талап етілетін қол жеткізу құқықтарын беру** – Қоғам қызметкерлері мен контрагенттерге еңбек міндеттерін және шарттық міндеттемелерді сапалы және уақтылы орындау үшін қажетті ең аз қолжетімділік құқығы қамтамасыз етіледі;

11) **Жобалық қызметте ақпараттық қауіпсіздік талаптарын есепке алу** - операциялық қызметтен басқа, Компания жобалық қызметте ақпараттық қауіпсіздік талаптарын ескеруге тырысады. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптарды әзірлеу және құжаттау ақпаратты өңдеуге, сақтауға және беруге байланысты жобаларды іске асырудың бастапқы кезеңдерінде жүзеге асырылады;

12) **Үздіксіздік** – Қоғамның ақпараттық қорғалуын қамтамасыз ету шаралары Қоғамның ағымдағы бизнес-процестерін тоқтатпай жүзеге асырылады;

13) **Толықтық** – ақпараттық ресурстарды пайдаланудың барлық технологиялық кезеңдерінде және барлық жұмыс режимдерінде олардың бүкіл өмірлік циклі бойына қауіпсіздігін қамтамасыз ету;

14) **Өзара әрекеттесу және үйлестіру** – ақпараттық қауіпсіздік шаралары Қоғамның тиісті құрылымдық бөлімшелерінің өзара қарым-қатынасы, алға қойылған мақсаттарға қол жеткізу үшін

олардың күш-жігерін үйлестіру, сондай-ақ сыртқы ұйымдармен қажетті байланыстарды орнату негізінде жүзеге асырылады.

15) **Қолайсыз факторлардың мақсаттарға әсерін бағалау** – ақпараттық технологияларда туындайтын немесе болжанатын кез келген қатерлер олардың қоғамның бизнес-процестерін орындаудың мақсаттары мен табыстылығына әсері бөлігінде бағалануы тиіс және қоғамның тәуекелдерін бағалауда көрініс табуы тиіс.

2.3.1. Қоғам заң талаптарына, сондай-ақ ақпараттық қауіпсіздік саласындағы халықаралық және ұлттық стандарттардың ережелері негізінде, ақпараттық қауіпсіздікті қамтамасыз ету бойынша ішкі нормативтік құжаттарды әзірлейді және енгізеді:

- ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шаралардың ұзақ мерзімді бағдарламасы;
- ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі ішкі нормативтік құжаттар;
- бизнестің үздіксіздігін қамтамасыз ету және төтенше жағдайлар кезіндегі әрекеттер жоспары.

2.3.2. Сонымен қатар, Қоғам мерзімді түрде ішкі нормативтік құжаттарға олардың тиімділігі мен дәйектілігі үшін талдау жасайды, сондай-ақ аталған құжаттарды жаңартылған күйінде сақтайды.

2.3.3. Осы Саясаттың ережелері Қоғамның ақпараттық-коммуникациялық инфрақұрылымы үшін сыртқы аудит жүргізу, ішкі талдау және ақпараттық қауіпсіздік саясаты ережелерінің талаптарын қозғайтын ақпараттандыру саласындағы заңнаманың және ақ кретикалық инциденттерінің өзгеруіне байланысты қайта қаралуға жатады. Саясат баяндалған ақпаратты талдау және жаңарту мақсатында (оны түзету қажеттілігін анықтау үшін) кемінде 2 (екі) жылда 1 (бір) рет қайта қаралады.

3. Ақпараттық қауіпсіздікті басқару жүйесінің қолданылу аясы

Қоғамда қабылданған Ақпараттық қауіпсіздік саясатының талаптарын егжей-тегжейлі көрсететін құжаттар:

- 1) ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі;
- 2) ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және таңбалау қағидалары;
- 3) Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі қағидалар;
- 4) есептеу техникасы, телекоммуникациялық жабдық және бағдарламалық қамтамасыз ету құралдарын түгендеу және паспорттау қағидалары;
- 5) АҚ ішкі аудитін жүргізу қағидалары;
- 6) ақпаратты криптографиялық қорғау құралдарын пайдалану қағидалары;
- 7) электрондық ақпараттық ресурстарға қол жеткізу құқықтарының аражігін ажырату қағидалары;
- 8) Интернет және электрондық поштаны пайдалану қағидалары;
- 9) аутентификация рәсімін ұйымдастыру қағидалары;
- 10) вирусқа қарсы бақылауды ұйымдастыру қағидалары;
- 11) мобильді құрылғылар мен ақпарат тасығыштарды пайдалану қағидалары;
- 12) ақпаратты өңдеу құралдарын және ақпараттық ресурстардың жұмыс істеуінің қауіпсіз ортасын физикалық қорғауды ұйымдастыру қағидалары;
- 13) ақпаратты резервтік көшіру және қалпына келтіру регламенті;
- 14) ақпараттық ресурстарға қашықтан қол жеткізуді ұйымдастыру қағидалары;
- 15) өнім берушілермен жұмыс кезінде ақпараттық қауіпсіздікті қамтамасыз ету қағидалары;
- 16) пайдаланушылардың АҚ инциденттеріне және штаттан тыс (дағдарыстық) жағдайларда ден қою жөніндегі іс-қимыл тәртібі туралы Нұсқаулық;
- 17) аспаптық тексеру жөніндегі жұмыстардың қағидалары;
- 18) ақпараттық қауіпсіздікті басқару;
- 19) ақпараттандыру объектісін сүйемелдеу жөніндегі әкімшінің басшылығы.

4. Жауапкершілік және міндеттемелер

4.1 Қоғам басшылығы:

– Қоғамның (бизнестің) мақсаттарына, заңдарға, нормативтік актілерге, Жарғыға және Қоғамның ішкі нормативтік құжаттарына сәйкес ақпараттық қауіпсіздікті қамтамасыз етуге қатысты мәселелерді шешуге қатысады;

– ақпараттық қауіпсіздік Қоғамның сәтті және тұрақты жұмысының маңызды факторларының бірі болып табылатынын біледі және қажетті көмек көрсетуге және ақпараттық қауіпсіздікті қамтамасыз етудің мақсаттары мен принциптерін жақтаушы екенін көрсетуге ниетті. Сондай-ақ Қоғам басшылығы ақпараттық қауіпсіздікті басқару процесін жалпы қадағалауды өзіне қалдырады;

– Қоғамның тиімді және тұрақты жұмысын қамтамасыз етуге, сондай-ақ барлық мүдделі тараптардың Қоғам жұмысының сенімділігі мен тұрақтылығына, олардың мүдделерін ақпараттық қауіпсіздік тәуекелдерінен қорғауға деген сенімін сақтауға ұмтылады;

– ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі ұйымдастырушылық және техникалық шаралардың теңгерімдеу кешеніне негізделген ақпараттық қауіпсіздікті басқару жүйесін құру, қолдау, бақылау және үздіксіз жетілдіру арқылы алға қойылған мақсатқа жетуге ұмтылады.

4.2 Ақпараттық қауіпсіздікке қатысты Қазақстан Республикасының заңдарын, стандарттарын және нормативтік талаптарын сақтамағаны үшін Қоғамның жұмыскерлеріне Қоғамның тиісті ішкі нормативтік құжаттарында, еңбек шарттарында және Қазақстан Республикасының қолданыстағы заңнамасында көзделген шаралар қолданылуы мүмкін, үшінші тұлғаларға шартта және Қазақстан Республикасының заңнамасында көзделген шаралар қолданылады.

4.3 Қоғамның барлық қызметкерлері Қазақстан Республикасының заңнамасына сәйкес қызметтік, коммерциялық немесе заңмен қорғалатын өзге де құпияны құрайтын мәліметтерді жария еткені, құжаттардың, осындай ақпаратты қамтитын ақпарат тасушыларының жоғалуы үшін жауапты болады.

4.4 Қоғамның ақпараттық қауіпсіздігіне және тәуекелдеріне жауапты атқарушы директор қауіпсіздікті басқарудың барлық аспектілеріне, соның ішінде осы Саясатты әзірлеуге, қайта қарауға, бағалауға, соның ішінде тәуекелдерді басқару бойынша шешім қабылдауға жауапты.

4.5 Процесс иелері ақпараттық қауіпсіздік құжаттамасын әзірлеуге, қайта қарауға, бағалауға жауапты.

4.6. Қоғам қызметкерлері міндетті:

1) ақпараттық жүйелердің қауіпсіздігін қамтамасыз ететін ішкі талаптарды білуге және сақтауға;

2) өз ақпаратының тұтастығын қамтамасыз ету үшін қолжетімді тіркелген қорғау тетіктерін пайдалануға;

3) орталық аппараттың/филиалдың тікелей басшысын, ішкі бақылау бағытындағы қызметкерлерді ақпараттық қауіпсіздіктің бұзылуы және өзге де күдікті жағдайлар мен оқыс оқиғалар туралы хабардар етуге міндетті;

4) Ақпараттық жүйелер ресурстарын қорғауда әлсіз жерлер анықталған жағдайда, бұл туралы ішкі бақылау бағытындағы қызметкерлерге дереу хабарлауға міндетті;

5) компьютерлік вирустың енуінің, анықталуының және жойылуының алдын алу үшін қажетті рәсімдерді орындауға міндетті;

6) қағаз құжаттарға, ауыспалы ақпараттық тасығыштарға және ақпаратты өңдеудің электрондық құралдарына қатысты "таза үстел" қағидатын сақтауға міндетті.