№ 546 от 25.06.2024



**«ҚазСтандарт» РМК-дағы**

**ақпараттық қауіпсіздік және**

**комплаенс туралы ережені бекіту туралы**

«Сыбайлас жемқорлыққа қарсы іс-қимыл туралы» 2015 жылғы 18 қарашадағы, «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы Қазақстан Республикасы Заңдарының, «Қазақстан Республикасының сыбайлас жемқорлыққа қарсы саясатының 2022 – 2026 жылдарға арналған тұжырымдамасын бекіту және Қазақстан Республикасы Президентінің кейбір жарлықтарына өзгерістер енгізу туралы Қазақстан Республикасы Президентінің 2022 жылғы 2 ақпандағы № 802 Жарлығының, «Квазимемлекеттік сектор субъектілеріндегі сыбайлас жемқорлыққа қарсы комплаенс-қызмет туралы үлгілік ережені бекіту туралы» Қазақстан Республикасы Сыбайлас жемқорлыққа қарсы іс-қимыл агенттігі Төрағасының 2023 жылғы 31 наурыздағы № 112 бұйрығының, «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысының, «ҚазСтандарт» РМК Жарғысының 4-бөлімі 22-тармағының 6) тармақшасының талаптарына және «ҚазСтандарт» республикалық мемлекеттік кәсіпорнында кадрлық қурамында жүргізілген өзгерістерге сәйкес **БҰЙЫРАМЫН:**

1. Қоса беріліп отырған «ҚазСтандарт» РМК-дағы Ақпараттық қауіпсіздік және комплаенс туралы ереже (бұдан әрі - Ереже) бекітілсін.

2. «ҚазСтандарт» РМК құрылымдық және аумақтық бөлімшелерінің басшыларын, қызметкерлерін 2024 жылғы 5 шілдеге дейин осы бұйрықпен таныстыру қамтамасыз етілсін (С.Қ. Арапов).

3. «ҚазСтандарт» РМК ІТ қызметі:

осы бұйрықты «ҚазСтандарт» РМК-ның ресми интернет-ресурсына орналастырсын;

Нұсқаулыкқа сәйкес «Сенім телефоны» ақпараттандыру арнасының жұмыс қабілеттілігін қамтамасыз етсін.

4. «ҚазСтандарт» РМК бас директордың орынбасарлары, құрылымдық бөлімшелердің басшылары және филиалдардың директорлары Ереже мен Қазақстан Республикасының сыбайлас жемқорлыққа қарсы заңнамасы талаптарының уақтылы және сапалы орындалуын қамтамасыз етсін.

6. «ҚазСтандарт» РМК сыбайлас жемқорлыққа қарсы қызметі туралы» «ҚазСтандарт» РМК Бас директорының 2021 жылғы 9 сәуірдегі бұйрығының 3, 4, 5-тармақтарының, «ҚазСтандарт» РМК сыбайлас жемқорлыққа қарсы комплаенс-қызметі туралы» «ҚазСтандарт» РМК Бас директорының
2023 жылғы 22 мамырдағы № 343 бұйрығының күші жойылды деп танылсын.

7. Осы бұйрықтың орындалуын бақылау «ҚазСтандарт» РМК ақпараттық қауіпсіздік және комплаенс жөніндегі менеджеріне жүктелсін.

8. Осы бұйрық қол қойылған күнінен күшіне енеді

**Бас директор м.а И.Хамитов**

 Қосымша

 «ҚазСтандарт» РМК Бас директоры м.а.

 2024 жылғы \_\_\_\_ маусымдағы №\_\_\_\_\_

 бұйрығына

 **«ҚазСтандарт» РМК-дегі ақпараттық қауіпсіздік**

**және комплаенс туралы ереже**

**1-тарау**

**Жалпы ережелер**

1.Осы «ҚазСтандарт» РМК-дағы ақпараттық қауіпсіздік және комплаенс туралы ереже (бұдан әрі – Ереже) «Сыбайлас жемқорлыққа қарсы іс-қимыл туралы» және «Ақпараттандыру туралы» Қазақстан Республикасы Заңдарының (бұдан әрі – Заң) талаптарына сәйкес әзірленді.

Ереже ақпараттық қауіпсіздік және комплаенс функцияларын орындайтын адамдардың мақсаттарын, міндеттерін, қағидаттарын, функциялары мен өкілеттіктерін айқындайды.

Ережеде мынадай негізгі ұғымдар қолданылады:

1) шабуыл – кіруді жою, ашу, өзгерту, шектеу, рұқсатсыз кіруді алу, ұрлау немесе ақпараттық активті рұқсатсыз пайдалану әрекеті;

2) бот - сақтандырушының ақпараттық жүйесінде берілген кесте және (немесе) алгоритм бойынша белгілі бір операцияларды автоматты түрде орындау үшін үшінші тұлғалар пайдаланатын бағдарламалық қамтамасыз ету;

3) кіру - ақпараттық активтерді пайдалану мүмкіндігі;

4) ақпараттық қауіпсіздік қатері - ақпараттық қауіпсіздіктің оқыс оқиғаларының пайда болуының алғышарттарын туындататын жағдайлардың және факторлардың жиынтығы;

5) ақпараттық жүйе – Кәсіпорынның деректері сақталатын және өңделетін ақпараттық жүйе;

6) ақпараттық-коммуникациялық инфрақұрылым - электрондық ақпараттық ресурстарды қалыптастыру және оларға қолжетімділік беру мақсатында технологиялық ортаның жұмыс істеуін қамтамасыз етуге арналған ақпараттық-коммуникациялық инфрақұрылым объектілерінің жиынтығы;

7) ақпараттық актив – ақпараттың және оны сақтауға және (немесе) өңдеуге пайдаланылатын ақпараттық-коммуникациялық инфрақұрылым объектісінің жиынтығы;

8) ақпараттық қауіпсіздіктің оқыс оқиғасы - ақпараттық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында жеке немесе сериялық туындайтын, олардың тиісінше жұмыс істеуіне қауіп келтіретін іркілістер және (немесе) Кәсіпорнының электрондық ақпараттық ресурстарын заңсыз алу, көшіру, тарату, модификациялау, жою немесе бұғаттауға арналған талаптар;

9) ақпараттық қауіпсіздікті қамтамасыз ету – Кәсіпорынның ақпараттық активтерінің конфиденциалдылық, тұтастық және қолжетімділік күйін ұстап тұруға бағытталған процесс;

10) ақпараттық-коммуникациялық инфрақұрылым объектілері – Кәсіпорынның ақпараттық жүйелері, технологиялық платформалар, аппараттық-бағдарламалық кешендер, телекоммуникация желілері, сондай-ақ техникалық құралдардың үздіксіз жұмыс істеуін қамтамасыз ету және ақпараттық қауіпсіздік жүйесі;

11) резервтік көшірме – қажет болған жағдайда оларды түпнұсқада немесе жаңадан орналастырылған орнында қалпына келтіруге арналған ақпарат тасымалдағыштағы деректер көшірмесі;

12) комплаенс (сыбайлас жемқорлыққа қарсы) – квазимемлекеттік сектор субъектілері мен оның қызметкерлерінің Қазақстан Республикасының сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі заңнамасын сақтауын қамтамасыз ету жөніндегі функция;

13) сыбайлас жемқорлық тәуекелдерін ішкі талдау – сыбайлас жемқорлық құқық бұзушылықтар жасауға ықпал ететін себептер мен жағдайларды анықтау және зерделеу;

14) мүдделер қақтығысы – жауапты мемлекеттік лауазымды атқаратын адамдардың, мемлекеттік функцияларды орындауға уәкілеттік берілген адамдардың, оларға теңестірілген адамдардың, лауазымды адамдардың жеке мүдделері мен олардың лауазымдық өкілеттіктері арасындағы қайшылық, мұндай жағдайда аталған адамдардың жеке мүдделері олардың өз лауазымдық міндеттерін орындамауына және (немесе) тиісінше орындамауына алып келуі мүмкін;

15) сыбайлас жемқорлық құқық бұзушылық – заңда әкімшілік немесе қылмыстық жауаптылық белгіленген, сыбайлас жемқорлық белгілері бар құқыққа қарсы кінәлі іс-әрекет (әрекет немесе әрекетсіздік);

16) сыбайлас жемқорлық тәуекелі – сыбайлас жемқорлық құқық бұзушылықтар жасауға ықпал ететін себептер мен жағдайлардың туындау мүмкіндігі;

17) сыбайлас жемқорлықтың алдын алу – сыбайлас жемқорлыққа қарсы іс-қимыл субъектілерінің алдын алу шаралары жүйесін әзірлеу және енгізу арқылы сыбайлас жемқорлық құқық бұзушылықтар жасауға ықпал ететін себептер мен жағдайларды зерделеу, анықтау, шектеу және жою жөніндегі қызметі;

18) сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі уәкілетті орган – Қазақстан Республикасының сыбайлас жемқорлыққа қарсы саясатын қалыптастыруды және іске асыруды және сыбайлас жемқорлыққа қарсы іс-қимыл саласындағы үйлестіруді, сондай-ақ сыбайлас жемқорлық құқық бұзушылықтардың алдын алуды, анықтауды, жолын кесуді, ашуды және тергеуді жүзеге асыратын мемлекеттік орган және оның аумақтық бөлімшелері.

2. «ҚазСтандарт» РМК-да ақпараттық функцияларды орындайтын жауапты тұлға болып ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер айқындалады. Бұл ретте ақпараттық қауіпсіздік және комплаенс функцияларын орындайтын жауапты тұлға ықтимал мүдделер қақтығысын ескере отырып айқындалады.

3. Ақпараттық қауіпсіздік және комплаенс функцияларын орындайтын жауапты тұлға (ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер) «ҚазСтандарт» РМК бас директорының шешімі негізінде тағайындалады.

4. Өкілеттігін жүзеге асыру кезінде ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер «ҚазСтандарт» РМК Бас директорына тікелей есеп береді, Қазақстан Республикасының сыбайлас жемқорлыққа қарсы іс-қимыл туралы заңнамасының талаптарын сақтауды қамтамасыз ету кезінде тәуелсіз болып табылады.

5. Ақпараттық қауіпсіздік және комплаенс (ақпараттық қауіпсіздік және комплаенс жөніндегі менеджердің) функцияларын «ҚазСтандарт» РМК басқа құрылымдық бөлімшелерінің функцияларымен ұштастыруға жол берілмейді.

**2-тарау.**

**Ақпараттық қауіпсіздік пен комплаенстің**

**(ақпараттық қауіпсіздік және комплаенс жөніндегі менеджердің)**

**мақсаттары, міндеттері, қағидаттары, функциялары мен өкілеттіктері**

8. Қызметтің негізгі мақсаты ақпараттық қауіпсіздік және сәйкестік жөніндегі менеджердің мынадай мақсаттары болып табылады:

-ақпараттық қауіпсіздік саласында – «ҚазСтандарт» РМК-да ақпараттық активтер мен ақпараттық қауіпсіздікті қорғауды қамтамасыз ету;

-сыбайлас жемқорлыққа қарсы іс-қимыл саласында – «ҚазСтандарт» РМК мен оның қызметкерлерінің Қазақстан Республикасының сыбайлас жемқорлыққа қарсы іс-қимыл туралы заңнамасын сақтауын қамтамасыз ету, сондай-ақ сыбайлас жемқорлыққа қарсы іс-шаралардың іске асырылуына мониторингті жүзеге асыру.

9. Ақпараттық қауіпсіздік және комплаенс (ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер) міндеттері мыналар:

-лауазымдық міндеттерді, жауаптылық салалары мен өкілеттіктерді бөлу арқылы ақпараттық қауіпсіздіктің ішкі ұйымдық құрылымын қалыптастыру;

-ақпараттық активтерге, ақпараттық жүйелерге қол жеткізуді бақылау;

-ақпараттық инфрақұрылымның үздіксіз жұмыс істеуін бақылау және қамтамасыз ету;

-қауіп-қатерлерге қарсы іс-қимыл және ақпараттық қауіпсіздіктің оқыс оқиғаларымен жұмыс;

-персоналға байланысты ақпараттық қауіпсіздік мәселелерін айқындау және ақпараттық қауіпсіздік саласындағы хабардарлықты арттыру;

-«ҚазСтандарт» РМК-ға және оның қызметкерлеріне сыбайлас жемқорлық құқық бұзушылықтардың ескерту және алдын алу құралдарын енгізуді қамтамасыз ету;

-«ҚазСтандарт» РМК-да сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі шаралар жүйесін тиімді іске асыру;

-«ҚазСтандарт» РМК-да сыбайлас жемқорлық тәуекелдеріне ішкі талдау жүргізуді қамтамасыз ету;

-сыбайлас жемқорлыққа қарсы іс-қимыл мәселелері бойынша сыртқы реттеуші талаптардың және үздік халықаралық практиканың сақталуын қамтамасыз ету;

-Қазақстан Республикасы қолданыстағы заңнамасына сәйкес сыбайлас жемқорлыққа қарсы іс-қимылдың негізгі қағидаттарының сақталуын қамтамасыз ету.

10. «ҚазСтандарт» РМК ақпараттық қауіпсіздік және комплаенс (ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер) функцияларын енгізу және жүзеге асыру кезінде мынадай қағидаттарды басшылыққа алады:

-ақпараттық қауіпсіздік және комплаенстің тиімділігіне басшылықтың мүдделілігі;

-ақпараттық қауіпсіздік және комплаенске функцияларын орындау үшін бөлінетін өкілеттіктер мен ресурстардың жеткіліктілігі;

-ақпараттық қауіпсіздік және комплаенс менеджерінің тәуелсіздигі;

-ақпараттық қауіпсіздік және комплаенс қызметінің ақпараттық ашықтығы;

-ақпараттық қауіпсіздік және комплаенс қызметі үздіксіз тәртіпте орындау;

-ақпараттық қауіпсіздік және комплаенсті үздіксіз жетілдіру.

 Ақпараттық қауіпсіздік қолданыс айясында:

-ақпараттық қауіпсіздік Қазақстан Республикасының қолданыстағы заңнамасының негізінде қамтамасыз етіледі;

-экономикалық орындылығы;

-артықшылықтарды барынша азайту;

-ақпараттандыру және дербес жауаптылық;

-өзара іс-қимыл және үйлестіру Кәсіпорынның тиісті құрылымдық бөлімшелерінің.

11. «ҚазСтандарт» РМК ақпараттық қауіпсіздік және комплаенс (ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер) функциялары:

Ақпараттық қауіпсіздік саласында

-мүдделі бөлімшелермен бірлесіп қызметтік, коммерциялық немесе заңмен қорғалатын өзге де құпияны құрайтын мәліметтер туралы ақпаратты және қорғалатын ақпаратпен жұмыс істеу тәртібін қамтитын қорғалатын ақпараттардың Тізбесін бекітуге енгізеді;

-қайта қарау тәртібі мен кезеңділігі ішкі құжаттармен айқындалатын ақпараттық қауіпсіздікті қамтамасыз ету процесін регламенттейтін ішкі құжаттарды бекітуге енгізеді;

-Кәсіпорынның құрылымдық бөлімшелері мен филиалдарының ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметін және қатерлерді анықтау және талдау, шабуылдарға қарсы іс-қимыл және ақпараттық қауіпсіздіктің оқыс оқиғаларын тергеу жөніндегі іс-шараларды ұйымдастырады, үйлестіреді және бақылауды жүзеге асырады;

-ақпараттық қауіпсіздікті қамтамасыз ету процесін қорғау жүйелерін қолдауды және әдіснамалық қолдауды ұйымдастырады;

-ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты жинауды, талдауды, шоғырландыруды, сақтауды және өңдеуді жүзеге асырады;

-Кәсіпорын қызметкерлерінің ақпараттық қауіпсіздік мәселелерінде хабардар болуын қамтамасыз ету жөніндегі іс-шараларды ұйымдастырады және жүргізеді;

-Кәсіпорын басшылығына ақпараттық қауіпсіздіктің жай-күйі туралы хабарлауды жүзеге асырады.

Сыбайлас жемқорлыққа қарсы іс-қимыл бойынша

-мыналарды әзірлеуді қамтамасыз етеді:

 -сыбайлас жемқорлыққа қарсы іс-қимылдың ішкі саясаты;

 -қызметкерлер үшін сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі нұсқаулық;

 -мүдделер қақтығысын анықтау және реттеудің ішкі саясаты;

 -сыбайлас жемқорлыққа қарсы іс-қимыл туралы заңнамаға сәйкес сыбайлас жемқорлыққа қарсы стандарт;

 -сыбайлас жемқорлыққа қарсы іс-қимыл мәселелері жөніндегі ішкі іс-шаралар жоспары;

 -қызметкерлердің сыбайлас жемқорлыққа қарсы заңнаманы бұзу фактілері немесе ықтимал бұзушылықтары туралы хабардар ету тәртібін регламенттейтін құжат;

 -корпоративтік әдеп пен мінез-құлық мәселелерін регламенттейтін құжат.

 Өз қызметі шеңберінде басқа сұрақтар бойынша

-сыбайлас жемқорлыққа қарсы саясаттың тиімділігіне қатысты ақпаратты жинауды, өңдеуді, қорытуды, талдауды және бағалауды жүзеге асырады;

-«Сыбайлас жемқорлық тәуекелдеріне ішкі талдау жүргізудің үлгілік қағидаларын бекіту туралы» Қазақстан Республикасы Мемлекеттік қызмет істері және сыбайлас жемқорлыққа қарсы іс-қимыл агенттігі Төрағасының 2016 жылғы 19 қазандағы №112 бұйрығымен бекітілген, Сыбайлас жемқорлық тәуекелдеріне ішкі талдау жүргізудің үлгілік қағидаларына сәйкес «ҚазСтандарт» РМК қызметінде сыбайлас жемқорлық тәуекелдеріне ішкі талдау жүргізуді үйлестіреді

-сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі уәкілетті орган және «ҚазСтандарт» РМК басшыларының бірлескен шешімі бойынша жүргізілетін «ҚазСтандарт» РМК қызметіне сыбайлас жемқорлық тәуекелдерін сыртқы талдауға қатысады;

-«ҚазСтандарт» РМК-да анықталған сыбайлас жемқорлық тәуекелдеріне және оларды митигациялау және жою жөнінде қабылданып жатқан шараларға мониторингті жүзеге асырады;

-«ҚазСтандарт» РМК-да сыбайлас жемқорлыққа қарсы іс-қимыл және сыбайлас жемқорлыққа қарсы мәдениетті қалыптастыру мәселелері бойынша түсіндіру іс-шараларын жүргізеді;

-«ҚазСтандарт» РМК қызметкерлері үшін сыбайлас жемқорлыққа қарсы оқыту семинарларын ұйымдастырады;

-«ҚазСтандарт» РМК қызметкерлерінің сыбайлас жемқорлыққа қарсы іс-қимыл саясатын және корпоративтік әдеп пен мінез-құлық мәселелерін сақтауын бақылауды қамтамасыз етеді;

-«ҚазСтандарт» РМК ұжымында жалпы қабылданған моральдық-этикалық нормаларға сәйкес келетін өзара қарым-қатынас мәдениетін қалыптастыруға жәрдемдеседі;

-ақпараттық қауіпсіздік және комплаенс жөніндегі менеджердің құзыреті шеңберінде мемлекеттік функцияларды орындауға уәкілеттік берілген тұлғаларға теңестірілген тұлғалардың Қазақстан Республикасының Сыбайлас жемқорлыққа қарсы іс-қимыл туралы заңнамасында белгіленген қаржылық бақылау шараларын және сыбайлас жемқорлыққа қарсы шектеулерді сақтауын қамтамасыз етеді;

-«ҚазСтандарт» РМК құрылымдық бөлімшелерінің сыбайлас жемқорлыққа қарсы іс-қимыл мәселелері жөніндегі ішкі іс-шаралар жоспарын орындауына мониторинг әзірлейді және жүргізеді;

-мүдделер қақтығысын, оның ішінде жұмысқа орналастыру, сатып алу және «ҚазСтандарт» РМК бизнес-процестер мәселелерін анықтау, мониторингілеу және реттеу жөнінде шаралар қабылдайды;

-«ҚазСтандарт» РМК сыйлықтар беру және алу мәселелерін реттеу жөнінде шаралар қабылдайды;

-контрагенттердің сенімділігін кешенді тексеруді жүзеге асырады;

-«ҚазСтандарт» РМК-да сыбайлас жемқорлық фактілері туралы өтініштер (шағымдар) негізінде қызметтік тексерулер жүргізеді және/немесе оларға қатысады;

-«ҚазСтандарт» РМК-да сыбайлас жемқорлыққа байланысты істер бойынша сыбайлас жемқорлыққа қарсы заңнамадағы, сот практикасындағы өзгерістерге мониторинг және талдау жүргізеді;

-«ҚазСтандарт» РМК құрылымдық бөлімшелері мен қызметкерлерінің сыбайлас жемқорлыққа қарсы шараларды іске асыру тиімділігіне бағалау жүргізеді;

-сыбайлас жемқорлыққа қарсы іс-қимыл мәселелері бойынша «ҚазСтандарт» РМК құрылымдық бөлімшелері мен қызметкерлерінің ақпаратын тыңдайды;

-«ҚазСтандарт» РМК Бас директорына анықталған сыбайлас жемқорлық тәуекелдерін жою, «ҚазСтандарт» РМК қызметін ұйымдастырудың ішкі процестерінің тиімділігін арттыру жөнінде ұсынымдар енгізеді;

-«ҚазСтандарт» РМК қызметінің ерекшелігіне қарай, егер мұндай функциялар тәуелсіздікке әсер етпесе және мүдделер қақтығысын тудырмаса, комплаенс, іскерлік әдебі, орнықты даму мәселелерімен байланысты функцияларды жүзеге асырады;

-сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі уәкілетті органмен және мемлекеттік органдармен, квазимемлекеттік сектор субъектілерімен, қоғамдық бірлестіктермен, сондай-ақ өзге де жеке және заңды тұлғалармен өзара іс-қимыл жасайды.

12. Ақпараттық қауіпсіздік және комплаенс жөніндегі менеджердің функционалдық міндеттері, құқықтары мен жауапкершілігі Ақпараттық қауіпсіздік және комплаенс-қызметтер туралы ереже негізінде әзірленетін лауазымдық нұсқаулықпен айқындалады және оны «ҚазСтандарт» РМК бас директоры бекітеді.

13.Ақпараттық қауіпсіздік және комплаенс құзыретіне кіретін мәселелер бойынша «ҚазСтандарт» РМК басқа құрылымдық бөлімшелеріне жіберілетін құжаттар мен сұрауларға ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер қол қояды.

14.Ақпараттық қауіпсіздік және комплаенс жөніндегі басшы мен қызметкерлер (менеджер) тиісті салаларда уәкілетті органдар мен кәсіптік ұйымдар өткізетін оқыту іс-шараларына қатысу жолымен кәсіби біліктілігін ұдайы арттыруы қажет.

15.Ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер өз қызметі шеңберінде:

-«ҚазСтандарт» РМК құрылымдық бөлімшелерінен ақпарат пен материалдарды, оның ішінде коммерциялық және қызметтік құпияны құрайтын материалдарды сұратады және алады;

-өз құзыретіне жататын мәселелерді «ҚазСтандарт» РМК Бас директорының қарауына шығаруға бастамашылық жасайды;

-ықтимал сыбайлас жемқорлық құқық бұзушылықтар, Қазақстан Республикасының ақпараттық қауіпсіздік және сыбайлас жемқорлыққа қарсы іс-қимыл туралы заңнамасын бұзушылықтар туралы келіп түсетін хабарламалар бойынша қызметтік тексерулер жүргізеді;

-«ҚазСтандарт» РМК басшылары мен басқа да қызметкерлерінен қызметтік тергеу шеңберінде жазбаша түсініктемелер беруді талап етеді;

-Қазақстан Республикасының Сыбайлас жемқорлыққа қарсы заңнамасын жетілдіру жөнінде ұсыныстар әзірлейді және оларды сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі уәкілетті органға жібереді;

-өз құзыреті шегінде ішкі құжаттардың жобаларын әзірлеуге қатысады;

-«ҚазСтандарт» РМК қызметкерлерінің «ҚазСтандарт» РМК-да сыбайлас жемқорлыққа қарсы заңнаманы бұзу фактілері немесе әлеуетті мүмкіндігі туралы хабарлауы не «ҚазСтандарт» РМК-ға сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі шаралардың тиімділігін арттыру жөнінде ұсыныстар енгізу үшін ақпараттандыру арналарын құрады;

16.Ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер өз қызметін жүзеге асыру кезінде:

-егер онда дайындалып жатқан және (немесе) жасалған сыбайлас жемқорлық құқық бұзушылық туралы деректер болмаса, «ҚазСтандарт» РМК және оның үлестес тұлғалары туралы ақпараттың, функцияларды жүзеге асыру кезеңінде белгілі болған инсайдерлік ақпараттың құпиялылығын сақтауға;

-«ҚазСтандарт» РМК-ға сыбайлас жемқорлықтың болжамды немесе нақты фактілері, әдеп кодексін бұзу және сыбайлас жемқорлыққа қарсы іс-қимыл мәселелері бойынша өзге де ішкі құжаттар бойынша жүгінген адамдардың құпиялылығын қамтамасыз етуге;

-«ҚазСтандарт» РМК Бас директорын ақпараттық қауіпсіздікті және сыбайлас жемқорлыққа қарсы заңнаманы бұзушылықтардың болуына немесе ықтимал мүмкіндігіне байланысты кез келген жағдайлар туралы хабардар етуге;

-дайындалып жатқан, жасалатын немесе жасалған сыбайлас жемқорлық құқық бұзушылықтардың белгілі болған жағдайлары туралы сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі уәкілетті органның назарына жеткізуге;

-«ҚазСтандарт» РМК белгіленген жұмыс режиміне кедергі келтірмеуге міндетті;

17.Ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер:

-алдыңғы үш жыл ішінде өзі қатысқан процестерді тексеруге қатыспауға;

-тексерудің әділдігіне нұқсан келтіруі немесе осындай нұқсан келтіруші ретінде қабылдануы мүмкін қызметке қатыспауға;

- құпия ақпаратты жеке мүддесі үшін пайдаланбауға;

-іскерлік әдеп нормаларын бұзбауға;

-нәтижесінде ақпараттық қауіпсіздік және комплаенс жөніндегі менеджердің тәуелсіздігіне, объективтілігіне және бейтараптығына залал келтіруі мүмкін не осындай залал келтіруші ретінде қабылдануы мүмкін сыйлықтарды қабылдамауға және көрсетілетін қызметтерді пайдаланбауға;

-тексерулерге, қызметтік тергеп-тексерулерге және мүдделер қақтығысына әкеп соғуы мүмкін басқа да ic-шараларға қатыспауға тиіс.

18. «ҚазСтандарт» РМК басшылығы:

-ақпараттық қауіпсіздік және комплаенс жөніндегі менеджердің қызметін жүзеге асыру үшін тиімді орта құруға ықпал ету, оның мақсаттарын, міндеттерін, функциялары мен міндеттемелерін орындауға, құқықтарын іске асыруға жәрдемдесуі;

-ақпараттық қауіпсіздік және комплаенс жөніндегі менеджердің қызметін әкімшілік (ұйымдастырушылық-техникалық) қамтамасыз етуді жүзеге асыруға, оның ішінде ақпараттық жүйелер мен қосымшаларды (қажетті дерекқорларға қолжетімділікті) және өзге де тауарларды, жұмыстарды, көрсетілетін қызметтерді қоса алғанда, оның қызметі үшін қажетті мүмкіндіктермен, активтермен және ресурстармен қамтамасыз етуі;

-ақпараттық қауіпсіздік және комплаенс жөніндегі менеджерге ақпараттық қауіпсіздік және комплаенс жөніндегі қызмет, әлеуметтік және коммуникациялық дағдылар мен құзыреттер мәселелері бойынша оқыту және сертификаттау мүмкіндіктерін беруі қажет.

19. Ақпараттық қауіпсіздік және комплаенс жөніндегі менеджердің «ҚазСтандарт» РМК құрылымдық бөлімшелерімен өзара іс-қимылы жұмыстағы өзара сыпайылық пен әдептілік негізінде құрылады.

20. «ҚазСтандарт» РМК құрылымдық бөлімшелерінің қызметкерлері ақпараттық қауіпсіздік және комплаенс жөніндегі менеджерге:

-квазимемлекеттік сектор субъектілеріндегі сыбайлас жемқорлыққа қарсы комплаенс-қызмет туралы үлгілік ереженің 14-тармағының
1) тармақшасында белгіленген бағыттардың ерекшеліктерін ескере отырып, ақпараттық қауіпсіздік және комплаенс жөніндегі менеджерге міндеттер мен функцияларды жүзеге асыру үшін қажетті құжаттар мен ақпаратты ұсыну;

-анықталған тәуекелдер мен бұзушылықтарды объективті талқылау;

-туындайтын мәселелер мен проблемаларды бірлесіп шешу арқылы жәрдемдеседі.

**З-тарау.**

**«ҚазСтандарт» РМК ақпараттық қауіпсіздік және комплаенс**

**жөніндегі менеджерінің есептілігі**

21.Ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер тоқсан сайын қабылданған сыбайлас жемқорлыққа қарсы шаралар бойынша ақпаратты сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі уәкілетті органға жібереді. Сыбайлас жемқорлыққа қарсы іс-қимыл жөніндегі уәкілетті органның сұрау салуы бойынша қабылданған сыбайлас жемқорлыққа қарсы шаралар бойынша қосымша ақпарат «ҚазСтандарт» РМК-ға жіберіледі.

22.Кәсiпорында ақпараттық қауiпсiздiк және комплаенс жөнiндегi менеджер белгiленген тәртiппен «ҚазСтандарт» РМК бас директорын ақпараттық қауiпсiздiк және комплаенс саласында қолданылып жатқан шаралар туралы хабардар етедi.

«ҚазСтандарт» РМК басшысы тарапынан ықтимал сыбайлас жемқорлық құқық бұзушылықтар туындаған кезде ақпараттық қауіпсіздік және комплаенс жөніндегі менеджер сәйкес уәкілетті мемлекеттік органдарға жүгінеді.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

****

**Об утверждении Положения об**

**информационной безопасности и**

**комплаенсе в РГП «КазСтандарт»**

В соответствии с требованиями Закона Республики Казахстан от 18 ноября 2015 года «О противодействии коррупции», от 24 ноября 2015 года «Об информатизации», Указа Президента Республики Казахстан от 2 февраля 2022 года N2802 «Об утверждении Концепции антикоррупционной политики Республики Казахстан на 2022 - 2026 годы и внесении изменений в некоторые указы Президента Республики Казахстан», приказа Председателя Агентства Республики Казахстан по противодействию коррупции от 31 марта 2023 года N2 112 «Об утверждении Типового положения об антикоррупционных комплаенс-службах в субъектах квазигосударственного сектора», постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», подпункта 6) пункта 22 раздела 4 Устава РГП «Казстандарт и в связи с кадровыми изменениями в составе РГП «КазСтандарт», **ПРИКАЗЫВАЮ**:

1. Утвердить прилагаемое Положение об информационной безопасности и комплаенс в РГП «КазСтандарт» (далее-Положение).

2. Обеспечить ознакомление руководителей, работников структурных и территориальных подразделений РГП «КазСтандарт» с данным приказом до 5 июля 2024 года (Арапов С.К.).

3. Службе IT РГП «КазСтандарт» обеспечить:

размещение настоящего приказа на официальном интернет-ресурсе РГП «КазСтандарт»;

обеспечить работу Единого телефона доверия в соответствии с Инструкцией.

4. Заместителям генерального директора, руководителям структурных подразделений и директорам филиалов РГП «КазСтандарт» обеспечить своевременное и качественное исполнение требований Положения и антикоррупционного законодательства Республики Казахстан.

5. Признать утратившими силу:

- пункты 3,4,5 приказа Генерального директора РГП «КазСтандарт» от 9 апреля 2021 года «Об антикоррупционной деятельности РГП «КазСтандарт»;

- приказ Генерального директора РГП «КазСтандарт» от 22 мая 2023 года №343 «Об утверждении Положение об антикоррупционном комплаенс-службе в РГП «КазСтандарт».

7. Контроль за исполнением настоящего приказа возложить на менеджера по информационной безопасности и комплаенс РГП «КазСтандарт».

8. Настоящий приказ вступает в силу со дня подписания.

**И.о. генерального директора И.Хамитов**

 Приложение

к приказу И.о.генерального директора

 РГП «КазСтандарт»

 от \_\_\_\_июня\_2024 года №\_\_\_\_\_

**Положение об информационной безопасности**

**и комплаенсе РГП «КазСтандарт»**

**Глава 1**

**Общие положения**

1.Настоящее Положение об информационной безопасности и комплаенсе в РГП «КазСтандарт» (далее — Положение) разработано в соответствии с требованиями Законов Республики Казахстан «О противодействии коррупции» и «Об информатизации» (далее — Закон).

Положение определяет цели, задачи, принципы, функции и полномочия лиц, исполняющих функции информационной безопасности и комплаенс.

В положении используются следующие основные понятия:

1)атака - попытка уничтожения, раскрытия, изменения, ограничения доступа, кражи, получения несанкционированного доступа или несанкционированного использования информационного актива;

2)бот - программное обеспечение, используемое третьими лицами для автоматического выполнения определенных операций по заданному расписанию и (или) алгоритму в информационной системе Предприятия;

3)доступ - возможность использования информационных активов;

 4)информационная безопасность - состояние защищенности электронных информационных ресурсов, информационных систем и информационной инфраструктуры от внешних и внутренних угроз;

5)информационная система - информационная система, в которой хранятся и обрабатываются данные Предприятия;

6)информационно-коммуникационная инфраструктура –совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

7)информационный актив - совокупность информации и объекта информационной- коммуникационной инфраструктуры, используемого для хранения и (или) обработки информации;

8)инцидент информационной безопасности - отдельно или серийно возникающие сбои в работе информационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов Предприятия;

9)обеспечение информационной безопасности - процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов Предприятия;

10)объекты информационной-коммуникационной инфра-структуры - информационные системы предприятия, технологические платформы, аппаратно-программные комплексы, сети телекоммуникаций, а также системы обеспечения бесперебойного функционирования технических средств и информационной безопасности;

11)резервная копия - копия данных на носителе информации, предназначенная для восстановления данных в оригинальном или новом месте их расположения в случае необходимости;

12) антикоррупционный комплаенс — функция по обеспечению соблюдения субъектами квазигосударственного сектора и его работниками законодательства Республики Казахстан по противодействию коррупции;

13)внутренний анализ коррупционных рисков — выявление и изучение причин и условий, способствующих совершению коррупционных правонарушений;

14)конфликт интересов- противоречие между личными интересами лиц, занимающих ответственную государственную должность, лиц, уполномоченных на выполнение государственных функций, лиц, приравненных к ним, должностных лиц и их должностными полномочиями, при котором личные интересы указанных лиц могут привести к неисполнению и (или) ненадлежащему исполнению ими своих должностных обязанностей;

15)коррупционное правонарушение - имеющее признаки коррупции противоправное виновное деяние (действие или бездействие), за которое законом установлена административная или уголовная ответственность;

16)коррупционный риск возможность возникновения причин и условий, способствующих совершению коррупционных правонарушений;

17)предупреждение коррупции — деятельность субъектов противодействия коррупции по изучению, выявлению, ограничению и устранению причин и условий, способствующих совершению коррупционных правонарушений, путем разработки и внедрения системы превентивных мер;

18)уполномоченный орган по противодействию коррупции — государственный орган, осуществляющий формирование и реализацию антикоррупционной политики Республики Казахстан и координацию в сфере противодействия коррупции, а также предупреждение, выявление, пресечение, раскрытие и расследование коррупционных правонарушений, и его территориальные подразделения.

2.Ответственным лицом, исполняющим функции информационной безопасности и комплаенса в РГП «КазСтандарт» определяется менеджер по информационной безопасности и комплаенсу. При этом ответственное лицо, исполняющее функции информационной безопасности и комплаенса, определяется с учетом потенциального конфликта интересов.

3.Ответственное лицо, исполняющее функции информационной безопасности и комплаенса (менеджер по информационной безопасности и комплаенсу), назначается на генеральным директором РГП «КазСтандарт».

4.При осуществлении полномочия менеджер по информационной безопасности и комплаенсу непосредственно подотчетен генеральному директору РГП «КазСтандарт», является независимым при обеспечении соблюдения требований законодательства Республики Казахстан о противодействии коррупции.

5.Не допускается совмещение функции информационной безопасности и комплаенса (менеджера по информационной безопасности и комплаенса) с функциями других структурных подразделений РГП «КазСтандарт».

**Глава 2.**

**Цели, задачи, принципы, функции и полномочия**

**информационной безопасности и комплаенса**

(менеджера по информационной безопасности и комплаенсу)

8.Основной целью деятельности менеджера по информационной безопасности и комплаенсу является:

*в области информационной безопасности:*

обеспечение защиты информационных активов и информационной безопасности в РГП «КазСтандарт»;

*в области противодействия коррупции:*

обеспечение соблюдения РГП «КазСтандарт» и его работниками законодательства Республики Казахстан о противодействии коррупции, а также осуществление мониторинга за реализацией мероприятий по противодействию коррупции.

9. Задачи информационной безопасности и комплаенса (менеджера по информационной безопасности и комплаенсу):

-формирование внутренней организационной структуры инфор-мационной безопасности, посредством распределения должностных обязанностей, сфер ответственности и полномочий;

-контроль доступа к информационным активам, информационным системам;

-контроль и обеспечение непрерывности функционирования информационной инфраструктуры;

-противодействие угрозам и работа с инцидентами информационной безопасности;

-определение вопросов информационной безопасности, связанных с персоналом и повышение осведомленности в области информационной безопасности;

-обеспечение внедрения инструментов предупреждения и превенции коррупционных правонарушений в РГП «КазСтандарт» и его работниками;

-эффективная реализация системы мер по противодействию коррупции в РГП «КазСтандарт»;

-обеспечение проведения в РГП «КазСтандарт» внутреннего анализа коррупционных рисков;

-обеспечение соблюдения внешних регуляторных требований и наилучшей международной практики по вопросам противодействия коррупции;

-обеспечение соблюдения основных принципов противодействия коррупции в соответствии с действующим законодательством РК.

10. РГП «КазСтандарт» при внедрении и осуществлении функций информационной безопасности и комплаенса (менеджер по информационной безопасности и комплаенс) руководствуется следующими принципами:

-заинтересованность руководства в эффективности информационной

безопасности и комплаенсу;

-достаточность полномочий и ресурсов, необходимых для выполнения задач по информационной безопасности и комплаенсу;

-независимость менеджера по информационной безопасности и комплаенсу;

-информационная открытость деятельности по информационной безопасности и комплаенсу;

-непрерывность осуществления деятельности по информационной безопасности и комплаенсу;

-совершенствование информационной безопасности и комплаенсу.

в области информационной безопасности:

обеспечени~~е~~ информационной безопасности на основе действующего законодательства РК;

экономическая целесообразность;

минимизация привилегий;

информированность и персональная ответственность;

взаимодействие и координация структурных подразделений Предприятия.

11.Функции информационной безопасности и комплаенса (менеджера по информационной безопасности и комплаенса) РГП «КазСтандарт»:

по вопросам информационной безопасности

-совместно с заинтересованными подразделениями вносит на утверждение Перечень защищаемой информации, включающий информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну, и порядок работы с защищаемой информацией;

-вносит на утверждение внутренние документы, регламентирующие процесс обеспечения информационной безопасности, порядок и периодичность пересмотра которых определяется внутренними документами;

-организует, координирует и осуществляет контроль деятельности структурных подразделений и филиалов Предприятия по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

-организует поддержку систем защиты и методологическую поддержку процесса обеспечения информационной безопасности;

-осуществляет сбор, анализ, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

-организует и проводит мероприятия по обеспечению осведомленности работников Предприятия в вопросах информационной безопасности;

-осуществляет информирование руководства Предприятия о состоянии информационной безопасности.

по вопросам противодействия коррупции

-обеспечивает разработку:

 -внутренней политики противодействия коррупции;

 -инструкции по противодействию коррупции для работников;

 -внутренней политики выявления и урегулирования конфликта интересов;

 -антикоррупционного стандарта, в соответствии с законодательством о противодействии коррупции;

 -внутреннего плана мероприятий по вопросам противодействия коррупции;

 -документа регламентирующего порядок информирования работниками о фактах или возможных нарушениях антикоррупционного законодательства;

 -документа, регламентирующего вопросы корпоративной этики и поведения;

по иным вопросам в пределах своей компетенции

-осуществляет сбор, обработку, обобщение, анализ и оценку информации, касающейся эффективности антикоррупционной политики;

-координирует проведение внутреннего анализа коррупционных рисков в деятельности РГП «КазСтандарт» в соответствии с Типовыми правилами проведения внутреннего анализа коррупционных рисков, утвержденными приказом Председателя Агентства Республики Казахстан по делам государственной службы и противодействию коррупции от 19 октября 2016 года N112 «Об утверждении Типовых правил проведения внутреннего анализа коррупционных рисков»;

-участвует во внешнем анализе коррупционных рисков в деятельности РГП «КазСтандарт», проводимом по совместному решению руководителей уполномоченного органа по противодействию коррупции и РГП «КазСтандарт»;

-осуществляет мониторинг выявленных коррупционных рисков в РГП «КазСтандарт» и принимаемых мер по их митигации и устранению;

-проводит разъяснительные мероприятия по вопросам противодействия коррупции и формированию антикоррупционной культуры в РГП «КазСтандарт»;

-организует антикоррупционные обучающие семинары для работников РГП «КазСтандарт»;

-обеспечивает контроль за соблюдением работниками РГП «КазСтандарт» политики противодействия коррупции и вопросов корпоративной этики и поведения;

-содействует формированию культуры взаимоотношений, соответствующей общепринятым морально-этическим нормам в коллективе РГП «КазСтандарт»;

-обеспечивает соблюдение лицами, приравненными к лицам, уполномоченным на выполнение государственных функций, мер финансового контроля и антикоррупционных ограничений, установленных законодательством о противодействии коррупции Республики Казахстан, в рамках компетенции менеджера по информационной безопасности и комплаенса;

-разрабатывает и проводит мониторинг исполнения структурными подразделениями РГП «КазСтандарт» внутреннего плана мероприятий по вопросам противодействия коррупции;

-принимает меры по выявлению, мониторингу и урегулированию конфликта интересов, в том числе в вопросах трудоустройства, закупок и бизнес-процессов РГП «КазСтандарт»;

-принимает меры по урегулированию вопросов дарения и получения подарков в РГП «КазСтандарт»;

-осуществляет комплексную проверку благонадежности контрагентов;

-проводит служебные проверки на основе обращений (жалоб) о фактах коррупции в РГП «КазСтандарт» и/или участвует в них;

-проводит мониторинг и анализ изменений в антикоррупционном законодательстве, судебной практики по делам, связанным с коррупцией в РГП «КазСтандарт»;

-проводит оценку эффективности реализации антикоррупционных мер структурными подразделениями и работниками РГП «КазСтандарт»;

-заслушивает информацию структурных подразделений и работников РГП «КазСтандарт» по вопросам противодействия коррупции;

-вносит генеральному директору РГП «КазСтандарт» рекомендации по устранению выявленных коррупционных рисков, повышению эффективности внутренних процессов организации деятельности РГП «КазСтандарт»;

-в зависимости от специфики деятельности РГП «КазСтандарт» осуществляет функции, связанные с вопросами комплаенс, деловой этики, устойчивого развития, если такие функции не влияют на независимость и не создают конфликта интересов;

-взаимодействует с уполномоченным органом по противодействию коррупции и государственными органами, субъектами квазигосударственного сектора, общественными объединениями, а также иными физическими и юридическими лицами.

12. Функциональные обязанности, права и ответственность менеджера по информационной безопасности и комплаенса определяются должностной инструкцией, разрабатываемой на основании Положения об информационной безопасности и комплаенс-службах и утверждается генеральным директором РГП «КазСтандарт».

13.Документы и запросы направляемые в другие структурные подразделения РГП «КазСтандарт» по вопросам, входящим в компетенцию информационной безопасности и комплаенс, подписываются менеджером по информационной безопасности и комплаенс.

14.Руководителю и работникам (менеджеру) по информационной безопасности и комплаенс необходимо постоянно повышать профессиональную квалификацию путем участия в обучающих мероприятиях, проводимых уполномоченными органами и профессиональными организациями в соответствующих областях.

15.Менеджер по информационной безопасности и комплаенс в пределах своей компетенции имеет право:

-запрашивать и получать от структурных подразделений РГП «КазСтандарт» информацию и материалы, в том числе составляющие коммерческую и служебную тайну;

-инициировать вынесение вопросов, относящихся к его компетенции, на рассмотрение Генеральному директору РГП «КазСтандарт»;

-проводить служебные проверки по поступающим сообщениям о возможных коррупционных правонарушениях, нарушениях законодательства Республики Казахстан об информационной безопасности и противодействии коррупции;

-требовать от руководителей и других работников РГП «КазСтандарт» представления письменных объяснений в рамках служебных расследований;

-разрабатывать предложения по совершенствованию анти-коррупционного законодательства Республики Казахстан и направлять их уполномоченному органу по противодействию коррупции;

-участвовать в разработке проектов внутренних документов в пределах своей компетенции;

-создавать каналы информирования для сообщения работниками РГП «КазСтандарт» о фактах наличия или потенциальной возможности нарушения антикоррупционного законодательства в РГП «КазСтандарт», либо внесения предложений по повышению эффективности мер по противодействию коррупции в РГП «Казстандарт»;

16.При осуществлении своей деятельности менеджер по информационной безопасности и комплаенс обязан:

 -соблюдать конфиденциальность информации о РГП «КазСтандарт» и его аффилированных лицах, инсайдерской информации, ставшей известной в период осуществления функций, если в ней не содержатся данные о готовящемся и (или) совершенном коррупционном правонарушении;

-обеспечивать конфиденциальность лиц, обратившихся по предполагаемым или фактическим фактам коррупции, нарушений кодекса этики и иных внутренних документов по вопросам противодействия коррупции в РГП «КазСтандарт»;

-информировать Генерального директора РГП «КазСтандарт» о любых ситуациях, связанных с наличием или потенциальной возможностью нарушений информационной безопасности и антикоррупционного законодательства;

-доводить до сведения уполномоченного органа по противодействию коррупции о ставших известными случаях готовящихся, совершаемых или совершенных коррупционных правонарушений;

-не препятствовать установленному режиму работы РГП «КазСтандарт»;

17.Менеджер по информационной безопасности и комплаенсу не должен:

-участвовать в проверках процессов, в которых он участвовали в течение предшествующих трех лет;

-участвовать в деятельности, которая могла бы нанести ущерб беспри

страстности проверки или восприниматься как наносящая такой ущерб;

-использовать конфиденциальную информацию в личных интересах;

-нарушать нормы деловой этики;

-принимать подарки и пользоваться услугами, в результате которых может быть нанесен ущерб независимости, объективности и беспристрастности менеджера по информационной безопасности и комплаенс либо которые могут восприниматься как наносящие такой ущерб;

-принимать участие в проверках, служебных расследованиях и других мероприятиях, которые могут привести к конфликту интересов.

18. Руководство РГП «КазСтандарт» необходимо:

-способствовать созданию эффективной среды для осуществления деятельности менеджера по информационной безопасности и комплаенса, оказывать содействие в выполнении его целям, задачам, функциям и обязанностям, в реализации прав;

-осуществлять административное (организационно-техническое) обеспечение деятельности менеджера по информационной безопасности и комплаенса, в том числе обеспечивать необходимыми для его деятельности возможностями, активами и ресурсами, включая, информационные системы и приложения (доступы к необходимым базам данных) и иными товарами, работами, услугами;

-предоставлять менеджеру по информационной безопасности и комплаенса возможности обучения и сертификации по вопросам деятельности по информационной безопасности и комплаенсу, социальных и коммуникационных навыков и компетенций.

19.Взаимодействие менеджера по информационной безопасности и комплаенса со структурными подразделениями РГП «КазСтандарт» строится на основе взаимной вежливости и корректности в работе.

20.Работники структурных подразделений РГП «КазСтандарт» оказывают менеджеру по информационной безопасности и комплаенсу содействие путем:

-предоставления документов и информации, необходимой для осуществления задач и функций менеджеру по информационной безопасности и комплаенсу, с учетом особенностей направления, в том числе установленных подпунктом 1) пункта 14 Типового положения об антикоррупционных комплаенс-службах в субъектах квазигосударственного сектора;

-объективного обсуждения выявленных рисков и нарушений;

-совместного решения возникающих вопросов и проблем.

**Глава З.**

**Отчетность менеджера по информационной**

**безопасности и комплаенсу РГП «КазСтандарт»**

21.Менеджер по информационной безопасности и комплаенсу ежеквартально направляет информацию по принятым антикоррупционным мерам в уполномоченный орган по противодействию коррупции. По запросу уполномоченного органа по противодействию коррупции направляется дополнительная информация по принятым антикоррупционным мерам в РГП «КазСтандарт».

22.Менеджер по информационной безопасности и комплаенсу в установленном порядке на предприятии, информирует генерального директора РГП «КазСтандарт» о принимаемых мерах в области информационной безопасности и комплаенс.

При возникновении возможных коррупционных правонарушений со стороны руководителя РГП «КазСтандарт» менеджер по информационной безопасности и комплаенсу обращается в уполномоченные государственные органы.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Согласовано**

25.06.2024 18:03 Копабаев Максат Боранбаевич

**Подписано**

25.06.2024 18:06 Хамитов И.В. ((и.о Амирханова Е.М.))

