

Техникалық қауіпсіздік

1. Жалпы ережелер

1.1. Осы "InfraTech" компаниясының техникалық қауіпсіздік саясаты (бұдан әрі — саясат) деректерді қорғаудың және сайттың қауіпсіз жұмыс істеуін қамтамасыз етудің негізгі шараларын айқындайды "infratech.kz" (бұдан әрі-Сайт).

1.2. Саясат сайттың жұмысына және пайдаланушылардың ақпаратын қорғауға әсер етуі мүмкін рұқсатсыз кіруді, деректердің бұзылуын және басқа қауіптерді болдырмауға бағытталған.

1.3. Компания Сайтта өзекті нұсқасын жариялай отырып, осы саясатқа өзгерістер енгізуге құқылы.

1.4. Пайдаланушылар саясаттағы өзгерістерді өз бетінше бақылауға міндетті.

1.5. Сайтты пайдалана отырып, Пайдаланушы осы Саясаттың шарттарын толық көлемде қабылдайтынын растайды. Кез-келген ережелермен келіспеген жағдайда, пайдаланушы сайтты пайдалануды тоқтатуы керек.

2. Деректер мен технологияларды қорғау

2.1. Компания деректерді қорғаудың заманауи әдістерін қолданады, соның ішінде:

- SSL/TLS көмегімен тасымалдау және сақтау кезінде деректерді шифрлау.
- Бағдарламалық жасақтама мен қорғаныс жүйелерін үнемі жаңартып отыру.
- Қауіптердің алдын алу үшін күдікті әрекеттерді бақылау және талдау.

2.2. Деректерге қол жеткізу тек компанияның уәкілетті қызметкерлерімен шектеледі.

2.3. Біз брандмауэр, антивирус және кірудің алдын алу жүйелері (IDS/IPS) сияқты көп деңгейлі қорғаныс жүйелерін қолданамыз.

3. Қол жеткізуді басқару

3.1. Компания пайдаланушы тіркелгілерін қорғау үшін көп факторлы аутентификацияны (MFA) енгізді.

3.2. Әрбір пайдаланушыға шифрлаумен қорғалған бірегей тіркелгі деректері ұсынылады.

3.3. Деректерге немесе жүйелерге рұқсатсыз кіру автоматты түрде бұғатталады.

4. Сақтық көшірме жасау және қалпына келтіру

4.1. Деректердің жоғалуын болдырмау үшін деректердің тұрақты сақтық көшірмесі жасалады.

4.2. Сақтық көшірмелер рұқсатсыз кіру мүмкін емес қорғалған аймақтарда сақталады.

4.3. Деректерді қалпына келтіру механизмдері күтпеген жағдайлар туындаған кезде жүйенің тоқтап қалу уақытын азайтуға мүмкіндік береді.

5. Осалдықтарды анықтау және жою

5.1. Компания ықтимал осалдықтарды анықтау үшін тұрақты қауіпсіздік аудиттерін жүргізеді.

5.2. Біз деректерді қорғауды тестілеу үшін кәсіби ұйымдармен жұмыс істейміз (мысалы, енуді тестілеу бағдарламалары арқылы — pentesting).

5.3. Қауіп анықталған жағдайда компания оны жою үшін дереу шаралар қабылдайды.

6. Қауіпсіздік үшін жауапкершілік

6.1. Біз ISO/IEC 27001, PCI DSS және басқаларын қоса алғанда, халықаралық қауіпсіздік стандарттарын ұстанамыз.

6.2. Компания өз қызметкерлерін ақпараттық қауіпсіздік мәселелеріне үнемі үйретеді.

7. Қауіпсіздік мәселелері туралы хабарлама

7.1. Егер сіз біздің сайтта осалдықты тапсаңыз немесе қауіпке күмәндансаңыз, бізге электрондық пошта арқылы хабарласыңыз: info@infratech.kz.

7.2. Қауіпсіздік мәселелері туралы барлық хабарламалар жедел қаралады және қажетті шаралар қысқа мерзімде қабылданады.

8. Саясаттағы өзгерістер

8.1. Техникалық қауіпсіздік саясаты жаңа стандарттар мен талаптарға сәйкес жаңартылуы мүмкін.

8.2. Саясаттың жаңартылған нұсқасы сайтта жарияланады және ол жарияланған сәттен бастап күшіне енеді.

9. Байланыс ақпараты

9.1. Техникалық қауіпсіздік сұрақтары үшін мына мекен-жайға хабарласыңыз: info@infratech.kz.

Біздің басты мақсатымыз — сайтты барлық пайдаланушылар үшін қауіпсіз және сенімді пайдалануды қамтамасыз ету.