«Халықаралық инженерлік-технологиялық университет» ЖШС		ТОО «Международный инженерно- технологический университет»
Ақпараттық технологиялар департаменті		Департамент информационных технологий
ЕРЕЖЕ		ПОЛОЖЕНИЕ
Ғылыми кеңес шешімімен бекітілді		Утверждено решением Ученого совета
№1 РЕДАКЦИЯСЫ		РЕДАКЦИЯ №1

Ақпараттық қауіпсіздік саясаты

Алматы, 2025

1. **Жалпы ережелер**
   1.1. Осы саясаттың мақсаты – Халықаралық инженерлік-технологиялық университетінің (бұдан әрі – ХИТУ) ақпараттық активтері мен студенттердің, оқытушылардың, қызметкерлердің және білім беру қызметімен байланысты басқа да тұлғалардың дербес деректерін қорғауға бағытталған ақпараттық қауіпсіздік талаптарын сақтауын қамтамасыз ету, сондай-ақ сенімгерлік немесе бақылаудағы басқарудағы заңды тұлғалардың мәліметтерін қорғау.
   1.2. Ақпаратты беру: дербес деректерді қамтитын ақпаратты беру кезінде жауапты тұлға оны қорғауды қамтамасыз ету үшін шифрлау әдісін – "парольмен шифрлау" немесе "парольдік қорғау" (Password Protection) әдісін қолданады.
   1.3. Тұтастық: бағдарламалық қамтамасыз етумен жұмыс істеу кезінде жауапты тұлғалар деректердің сапасын – ақпараттың дәлдігін, толықтығын және өзгеріссіздігін қамтамасыз етеді.
   1.4. Қолжетімділік: ақпаратты өңдеу барысында жауапты тұлғалар оны қажет пайдаланушыларға рұқсат етілген қолжетімділікті қамтамасыз ету үшін жүйелі тәсілдерді қолданады.
2. **Негізгі міндеттер мен компоненттер**
   2.1. Ақпараттық активтерді сәйкестендіру: аппараттық-техникалық құралдар мен бағдарламалық жасақтаманың құрамында бар деректерді, соның ішінде дербес деректерді анықтау.
   2.2. Ақпараттық қауіпсіздік бойынша кешенді шаралар: ақпараттық активтерге қауіп-қатерлерді анықтау, ақпаратты қорғау шараларын енгізу, қорғаныс жүйесінің тиімділігін тұрақты түрде тексеру.
   2.3. Дербес деректерді өңдеуге жауапты тұлғаны тағайындау (бұдан әрі – Деректерді қорғау бойынша жауапты тұлға).
   2.4. Деректерді сәйкестендіру және жинау бойынша өкілетті тұлғалар мен бөлімдерді анықтау.
   2.5. Жұмысшылар мен басқа тұлғалардың ақпаратпен жұмыс істеу функционалдық міндеттерін, өкілеттіктерін және жауапкершілік шараларын анықтау.
   2.6. Ақпараттық қауіпсіздік ережелері мен рәсімдерін әзірлеу.
   2.7. Техникалық қорғау, шифрлау жүйелері, қолжетімділікті бақылау, деректердің резервтік көшірмесін жасау және инциденттерді басқару бойынша ұйымдастырушылық шараларды әзірлеу.
3. **Деректерді қорғау бойынша жауапты тұлға**
   3.1. Қазақстан Республикасының "Дербес деректер және оларды қорғау туралы" заң талаптарын орындайды.
   3.2. Қызметкерлерден, оның ішінде ХИТУ-дың жоғары басшылығынан, дербес деректерді қорғау бойынша шараларды жүзеге асыруды талап етуге құқылы.
   3.3. ХИТУ және оның қызметкерлері тарапынан дербес деректерді қорғау заңнамасының сақталуын ішкі бақылауды жүзеге асырады.
   3.4. Дербес деректерді қорғау мәселелері бойынша Қазақстан Республикасы заңнамасының талаптарын ХИТУ қызметкерлеріне жеткізеді.
   3.5. Дербес деректерге қатысты шағымдар мен сұраныстарды қабылдау және өңдеуді бақылайды.
   3.6. Деректерді сәйкестендіру, жинау, өңдеу, сақтау және жою бойынша регламенттерді әзірлейді.
   3.7. Уәкілетті мемлекеттік органдар тарапынан жүргізілетін тексерулерге жәрдемдеседі.
   3.8. Дербес деректер тізімін анықтап, оны уәкілетті органда бекітеді.
   3.9. Дербес деректерді қорғау шараларын іске асыру үшін бизнес-процестерді ұйымдастырады, деректерді аппараттық-техникалық құралдар мен бағдарламалық

қамтамасыз ету, деректер қоймасы және аналитикалық есептер арасында беру қауіпсіздігін қамтамасыз етеді.

3.10. Дербес деректердің таралуын бақылау мақсатында корпоративтік коммуникация құралдары немесе электрондық құжат айналымы жүйесі арқылы тапсырыс беруші мен орындаушы арасындағы сұраулар мен аналитикалық ақпарат алмасуын жүйелендіреді.

4. Басшылық

4.1. Ақпараттық қауіпсіздік саясатының тиімді іске асырылуын қадағалайды.
4.2. Ақпараттық қауіпсіздік бастамаларын нақты басқарады және қолдайды.
4.3. Ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ресурстарды бөледі.
4.4. Ақпараттық қауіпсіздікке жауапты бөлімдер мен қызметкерлердің рөлдері мен міндеттерін лауазымдық нұсқаулықтар, бұйрықтар мен ережелер арқылы бекітеді.
4.5. Ақпараттық қауіпсіздік саясатын бұзған жағдайда тәртіптік шаралар қолданады.

5. Қызметкерлер және басқа тұлғалар

5.1. Деректерді қорғау бойынша жауапты тұлғаның талаптарын орындайды.
5.2. Дербес деректерді сәйкестендіру, жинау, өңдеу, сақтау және жою бойынша регламенттерді әзірлейді.
5.3. Дербес деректерді қорғау талаптарын бұзған жағдайда жеке жауапкершілік көтереді, соның ішінде корпоративтік электрондық поштасы, компьютерлері, жеке аккаунттары, мессенджерлері және басқа да коммуникация құралдарындағы ақпараттың қауіпсіздігі үшін жауапты.
5.4. Деректерді қорғау бойынша жауапты тұлғаға бұзушылықтар туралы хабарлайды.
5.5. Аппараттық-техникалық құралдар мен бағдарламалық қамтамасыз етудегі деректер сапасына жауапты болады, сәйкессіздіктерді анықтап, оларды түзету бойынша шаралар қабылдайды.

6. Ақпараттық қауіпсіздікке жауапты қызметкерлер мен бөлімдер

6.1. Ақпараттық қауіпсіздік жүйесін әзірлеуге, енгізуге және жетілдіруге жауапты.
6.2. IT-инфрақұрылымының жағдайын, серверлерді, желілерді, деректер сақтау жүйелерін және бағдарламалық қамтамасыз етуді бақылауды жүзеге асырады.
6.3. Жүйелер мен процестердің осалдықтары мен тәуекелдерін анықтау үшін тұрақты аудит жүргізеді.
6.4. Ақпараттық ресурстарға, оның ішінде тіркелгілерге, құпиясөздерге және желілік ресурстарға қолжетімділікті бақылайды.
6.5. Ақпараттық қауіпсіздік саясаты мен ішкі нормативтік құжаттардың сақталуын қамтамасыз етеді.
6.6. Қызметкерлерді ақпараттық қауіпсіздік ережелері туралы ақпараттандыру үшін материалдар (буклеттер, жадынамалар) әзірлейді.
6.7. Барлық қызметкерлерге тұрақты оқыту және нұсқаулықтар өткізеді.

7. Ақпаратты қорғау объектілері

7.1. ХИТУ-дағы ақпараттық қауіпсіздікті қамтамасыз етудің негізгі объектілері мыналар болып танылады:

7.1.1. **Ақпараттық ресурстар:**

7.1.1.1. Деректер: дербес деректер, қаржылық ақпарат, коммерциялық құпиялар, зияткерлік меншік және т.б.
7.1.1.2. Бағдарламалар: операциялық жүйелер, қолданбалы бағдарламалық қамтамасыз ету, дерекқорлар.
7.1.1.3. Құжаттама: техникалық құжаттама, нұсқаулықтар, пайдаланушы жөніндегі нұсқаулықтар.

7.1.2. **Ақпараттық жүйелер:**

7.1.2.1. Компьютерлер мен серверлер.
7.1.2.2. Желілер: жергілікті және ғаламдық желілер.

7.1.2.3. Деректерді сақтау жүйелері.
7.1.2.4. Байланыс құралдары.
7.1.3. **Физикалық объектілер:**
7.1.3.1. Ғимараттар, құрылыстар, бөлмелер.
7.1.3.2. Жабдықтар: компьютерлер, серверлер, желілік жабдықтар, бейнебақылау және кіруді бақылау жүйелері.
7.1.3.3. Ақпарат тасымалдаушылар: қатты дискілер, флеш-жинақтауыштар, оптикалық дискілер.
7.1.4. **Бағдарламалық қамтамасыз ету:**
7.1.4.1. Platonus
7.1.4.2. AIS METU
7.1.4.3. 1C
7.1.4.4. HikCentral (СКУД)
7.1.4.5. Деректер қоймасы
7.1.4.6. Thunderbird пошта клиенті (немесе пошта бағдарламасы)
7.1.4.7. Басқа бағдарламалар.

8. Ақпараттық жүйелерді пайдалану шектеулері мен талаптары

8.1. Корпоративтік поштаға қол жеткізу
8.1.1. Корпоративтік хат алмасудың құпиялылығы мен қауіпсіздігін қамтамасыз ету мақсатында корпоративтік пошта жәшіктеріне қол жеткізу үшін тек бекітілген корпоративтік пошта клиентін пайдалану қажет.
8.1.2. Басқа браузерлер мен пошта серверінің веб-интерфейстерін пайдалану құпия ақпараттың таралуына және ақпараттық қауіпсіздік саясатының бұзылуына әкелуі мүмкін.
8.2. Белсенді каталог жүйесі (Active Directory)
8.2.1. Университеттің барлық жұмыс станциялары бірыңғай белсенді каталог жүйесіне (Active Directory) қосылған. Бұл пайдаланушылардың корпоративтік ресурстарға қол жеткізуін орталықтандырылған түрде басқаруға, бірыңғай құпиясөз саясатын қамтамасыз етуге және пайдаланушылар әрекеттерін аудиттеуге мүмкіндік береді.
8.3. Антивирустық қорғаныс және құрылғыларды бақылау
8.3.1. Университеттің барлық жұмыс станцияларында компьютер мен ондағы ақпаратты ықтимал қауіптерден қорғау үшін антивирустық бағдарламалық қамтамасыз ету орнатылуы тиіс.
8.3.2. Антивирустық бағдарламалық жасақтама автоматты түрде жаңартылып, жүйені тұрақты түрде зиянды бағдарламаларға тексеретіндей бапталуы қажет.
8.4. Желіні сегменттеу
8.4.1. Корпоративтік жергілікті желі сыртқы желілерден қатаң оқшаулануы тиіс. Корпоративтік желіге жеке құрылғыларды (смартфондар, планшеттер) ақпараттық қауіпсіздік әкімшісінің алдын ала мақұлдауынсыз қосуға тыйым салынады.
8.4.2. Корпоративтік желіні өндірістік қызметке қатысы жоқ сыртқы ресурстарға кіру үшін пайдалануға болмайды.
8.5. Интернет-гигиена қағидалары
8.5.1. Барлық қызметкерлер интернет-гигиена қағидаларын сақтауы тиіс. Негізгі қағидаларға мыналар жатады:
8.5.1.1. Электрондық хаттардағы күмәнді тіркемелерді ашпау.
8.5.1.2. Белгісіз көздерден алынған сілтемелерге өтпеу.
8.5.1.3. Әкімші рұқсатынсыз жұмыс станцияларына бағдарламалық қамтамасыз етуді орнатпау.
8.5.1.4. Қоғамдық Wi-Fi желілерін корпоративтік ресурстарға кіру үшін пайдаланбау.

8.5.1.5. Жеке тіркелгі деректерін үшінші тұлғаларға бермеу.

8.6. Қашықтан жұмыс істеу

8.6.1. Қашықтан жұмыс істеу кезінде қауіпсіздік талаптарын реттейтін жеке құжат әзірленуі тиіс.

8.7. Электрондық құжат айналымы жүйесімен (ЭҚАЖ) жұмыс істеу

8.7.1. Сыртқы платформа болып табылатын ЭҚАЖ-де жұмыс істеу кезінде келесі ережелерді сақтау қажет:

8.7.1.1. Құпия ақпарат: Құпия деректері бар барлық ақпарат ЭҚАЖ-ге жүктелмес бұрын мұрағатталып, парольмен қорғалуы тиіс. Әрбір құжат немесе құжаттар топтамасы үшін күрделі және бірегей пароль орнату қажет.

8.7.1.2. Қолжетімділік: ЭҚАЖ-ге тек жүйеде жеке тіркелген пайдаланушылар ғана қол жеткізе алады.

8.7.1.3. Көшірмелер: Құпия ақпарат бар құжаттардың жергілікті көшірмелерін жасау тек қызметтік қажеттілік болған жағдайда және тікелей басшының рұқсатымен жүзеге асырылады.

8.7.1.4. Деректерді бейтараптандыру: Барлық құпия ақпарат дербес деректердің орнына бірегей идентификаторларды (мысалы, ID, қызметкердің табельдік нөмірі) қолдану арқылы бейтараптандырылуы тиіс.

9. Тұлғаларды идентификациялау

9.1. Тұлғаларды сәйкестендіруге қойылатын талаптар

9.1.1. Жеке басын растау: Сәйкестендіру тек ресми құжаттар негізінде жүргізілуі тиіс (жеке куәлік, паспорт және т.б.).

9.1.2. Жеке деректерді өңдеуге рұқсат: Жеке тұлғаның деректерін өңдеу үшін оның жазбаша келісімі алынуы қажет.

9.1.3. Өкілеттілік: Сәйкестендіруді тек қызметтік нұсқаулықтар мен құрылымдық бөлімше ережелеріне сәйкес өкілеттілігі бар қызметкерлер жүргізе алады.

9.1.4. Әрекеттерді журналға тіркеу: Жеке деректерді енгізу, өзгерту және жою бойынша барлық операциялар аудит журналында тіркелуі тиіс.

10. Ақпараттық жүйелерге қолжетімділік

10.1. Қолжетімділік деңгейлері:

10.1.1. Толық қолжетімділік – жүйе әкімшілеріне беріледі, олар жүйені баптау, қызмет көрсету және басқа пайдаланушылардың қолжетімділігін басқару бойынша барлық операцияларды орындауға құқылы.

10.1.2. Шектеулі қолжетімділік – қарапайым пайдаланушыларға беріледі және тек олардың қызметтік міндеттерін орындау үшін қажетті функцияларды ғана орындауға мүмкіндік береді.

10.2. Қолжетімділікті беру негіздері:

10.2.1. Лауазымдық нұсқаулық – қолжетімділік беру негізі қызметкердің лауазымдық нұсқаулығы болып табылады, онда оның қызметтік міндеттері мен қажетті ақпараттық ресурстар нақты көрсетілген.

10.2.2. Қолжетімділікті беру туралы өтінім – қызметкер қолжетімділікті алу үшін тікелей басшысы мақұлдаған тиісті өтінімді толтыруы қажет.

10.2.3. Қолжетімділікті беру туралы шешім – қолжетімділікті беру туралы шешімді ұйым басшысының бұйрығымен тағайындалған жауапты тұлға қабылдайды.

10.3. Қолжетімділікті беру рәсімі:

10.3.1. Идентификация және аутентификация – қолжетімділік берер алдында қызметкер өзінің жеке басы мен өкілеттіктерін растау үшін сәйкестендіру және аутентификациядан өтуі тиіс.

10.3.2. Пайдаланушы тіркелгісін жасау – тағайындау немесе қолжетімділікті беру туралы бұйрық/шешім негізінде пайдаланушы тіркелгісі жасалады және оған бірегей идентификатор мен құпиясөз беріледі.

10.3.3. Рөлдер мен құқықтарды тағайындау – пайдаланушыға оның лауазымдық міндеттеріне сәйкес қолжетімділік деңгейі мен рөлі беріледі.

10.4. Қолжетімділікті қайтарып алу:

10.4.1. Қызметкер жұмыстан шыққанда – ақпараттық жүйелерге қолжетімділік қызметкер жұмыстан шыққан күні жойылады.

10.4.2. Лауазымдық міндеттердің өзгеруі кезінде – қызметкердің лауазымдық міндеттері өзгерген жағдайда, оның қолжетімділік құқықтары қайта қаралуы тиіс.

10.4.3. Ақпараттық қауіпсіздік саясатын бұзу кезінде – егер қызметкер ақпараттық қауіпсіздік саясатын бұзса, оның ақпараттық жүйелерге қолжетімділігі шектелуі немесе толығымен жойылуы мүмкін.

10.5. Қолжетімділік құқықтарын мерзімді қайта қарау:

Ұйым құрылымы немесе қызметкерлердің лауазымдық міндеттері өзгерген кезде пайдаланушылардың қолжетімділік құқықтарын тұрақты түрде қайта қарау ұсынылады.

10.6. Пайдаланушылардың белсенділігін бақылау:

Ақпараттық жүйелерде күдікті әрекеттерді анықтау үшін пайдаланушылардың белсенділігін үнемі бақылау қажет.

11. Қорытынды ережелер

11.1. Осы саясаттың талаптарын және Қазақстан Республикасының дербес деректер туралы заңнамасын бұзған тұлғалар ішкі нормативтік құжаттар мен қолданыстағы заңнамаға сәйкес жауапкершілікке тартылады.

11.2. Осы Ереже бекітілген сәттен бастап күшіне енеді және оны өзгерту немесе жою сәтіне дейін қолданылады.

11.3. Тұрақты тексерулер және жаңартулар: Бұл саясат заңнамадағы өзгерістер мен ақпараттық қауіпсіздікке төнетін жаңа қауіптерге байланысты тұрақты түрде қайта қаралып, жаңартылып отыруы қажет.

11.4. Жауапкершілік және санкциялар: Осы Саясаттың кез келген тармағын бұзған немесе талаптарды тиісінше орындамаған қызметкерлерге тәртіптік жаза қолданылуы мүмкін, сондай-ақ сыйақылардан, бонустардан немесе еңбекақыға қосылатын үстемақылардан айыру шаралары қарастырылуы мүмкін.

12. Бекітуге жауапты тұлға

12.1. *Ақпараттық технологиялар департаменті директоры*: *Шындалы С. Б.*

*Құжатты бекіту үшін жауапты тұлғаның қолы*_____