БЕКІТЕМІН
«Жұмабек Ахметұлы Тәшенев атындағы университетінің» АҚ
Ректоры
_____ Қ.С.Байболов
_____ 2025 жыл

САПА МЕНЕДЖМЕНТ ЖҮЙЕСІ

САЯСАТ

УЕ-59-25

ЖҮЙЕЛЕРДІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН ЖӘНЕ ДЕРЕКТЕРДІ ҚОРҒАУДЫ ҚАМТАМАСЫЗ ЕТУ

1. Цифрлық даму орталығымен ӘЗІРЛЕНДІ ЖӘНЕ ЕНГІЗІЛДІ
2. Әзірлегендер – Цифрлық даму орталығының басшысы Шпенглер С.А.

3. Келісілді
   - Басқарма мүшесі – Аппарат басшысы Сугирбекова К.С.
   - HR Департаментінің Директоры Маликова А.А.
   - Заң қызметінің басшысы Ильясов Р.М.
   - Сапа менеджменті жүйесі бөлімінің басшысы Тауасарова А.С.

4. Жұмабек Ахметұлы Тәшенев атындағы университеттің Ғылыми Кеңесінің отырысында талқыланып, мақұлданды № 3 30.09 2025 жылы

5. Енгізілді – 2025
6. Тексерілу мерзімі – 2027

Қызмет бабында пайдаланатын басылым

Шымкент, 2025

МАЗМҰНЫ

1. ЖАЛПЫ ЕРЕЖЕЛЕР

«Жұмабек Ахметұлы Ташенев атындағы университет» АҚ-ның (бұдан әрі – Университет) осы ақпараттық қауіпсіздік саясаты (бұдан әрі - Саясат) Қазақстан Республикасының қолданыстағы заңнамасына, Университет ережелеріне және басқа да ішкі ережелеріне сәйкес әзірленді.

Осы Саясат құпия ақпараттың келесі анықтамасын қолданады: «Құпия ақпарат» дегеніміз пайдаланушылардың жеке деректеріне, бағдарламалық өнімдер дерекқорларындағы деректерге, сондай-ақ Университет пен оның контрагенттерінің қызметіне, біліміне, ноу-хауына, коммерциялық ақпаратына және баға белгілеуіне қатысты кез келген және барлық ақпарат, олар қызметкерге олардың жұмысы нәтижесінде белгілі болған кез келген жолмен.

Университеттің ақпараттық қауіпсіздік саясаты ақпараттық активтерді Университеттің материалдық активтері ретінде кездейсоқ немесе қасақана өзгертуден, жария етуден немесе жоюдан қорғау, сондай-ақ ақпараттың құпиялылығын, тұтастығын және қолжетімділігін сақтау, сондай-ақ тұтынушылар мен серіктестермен ақпарат алмасуды қамтамасыз ету үшін қажетті шараларды көздейді.

Университеттің әрбір қызметкері ақпараттық қауіпсіздікті сақтауға жауапты. Қызметкерлер өздерінің қызметтік міндеттерін орындау үшін қажетті ақпаратқа уақтылы және толық қол жеткізуі керек.

Осы Саясаттың мақсаттары үшін келесі терминдер мен анықтамалар қолданылады:

– Ақпараттық қауіпсіздік — оның құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ететін ақпараттық қауіпсіздік жағдайы.

– Құпиялылық — белгілі бір тұлғалар үшін оған қол жеткізуді шектейтін ақпараттың қасиеті.

– Тұтастық — ақпараттың өңдеу кезінде оның сенімділігі мен өзгермейтіндігінен тұратын қасиеті.

– Қолжетімділік — ақпараттың қажетті уақытта және қажетті жерде мақсатты мақсаты үшін пайдалану мүмкіндігінен тұратын қасиеті.

– Ақпараттық қауіпсіздікке төнген қатер — ақпараттық қауіпсіздіктің бұзылуының ықтимал немесе нақты қаупін тудыратын жағдайлар мен факторлар жиынтығы.

– Ақпараттық қауіпсіздіктің осалдығы – ақпараттық қауіпсіздікті бұзу үшін пайдаланылуы мүмкін қажетті қорғаныс деңгейінің жетіспеушілігі немесе болмауы.

– Ақпараттық қауіпсіздік тәуекелі – ақпараттық қауіпсіздікке төнген қатер ықтималдығы мен ықтимал залал мөлшерінің үйлесімі.

– Тәуекелдерді басқару процестері – ақпараттық қауіпсіздік тәуекелдерін анықтауға, бағалауға және азайтуға бағытталған тізбекті әрекеттер жиынтығы.

– Жаңартулар – бағдарламалық жасақтамаға, бағдарламалық жасақтамаға немесе аппараттық құралға қателерді түзету, осалдықтарды жою немесе жаңа мүмкіндіктерді қосу үшін енгізілген өзгерістер.

Осы Саясатта «қызметкер» термині Университеттің барлық қызметкерлеріне, соның ішінде азаматтық-құқықтық келісімшарттар бойынша Университетте жұмыс істейтіндерге қатысты. Осы Саясаттың қолданылуы осындай келісімшарттарда көрсетілуі тиіс.

Ақпараттық қауіпсіздік Университет қызметінің маңызды аспектісі болып табылады. Ұйым ақпараттың құпиялылығын, тұтастығын және қолжетімділігін, сондай-ақ деректерді рұқсатсыз кіруден, пайдаланудан, жария етуден, өзгертуден, жоюдан немесе жоғалтудан қорғауды қамтамасыз етуге тырысады.

Бұл Саясат әрбір Университет қызметкеріне еңбек шарты жасалған күні жеткізілуі тиіс.

2. НОРМАТИВТІК СІЛТЕМЕЛЕР МЕН АНЫҚТАМАЛАР

Өз қызметінде Саясат төмендегі құқықтық базаға сүйенеді:

2.1. Сыртқы нормативтік-құқықтық актілер:

– Қазақстан Республикасының Конституциясы;

– Қазақстан Республикасының Азаматтық кодексі;

– Қазақстан Республикасының Еңбек кодексі;

– Қазақстан Республикасының «Білім туралы», «Дербес деректер және оларды қорғау туралы», «Қазақстан Республикасының Цифрлық кодексі», «Ақпараттандыру туралы», «Ғылым және технологиялық саясат туралы», «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы», «Қазақстан Республикасындағы тілдер туралы», «Мемлекеттік жастар саясаты туралы», «Акционерлік қоғамдар туралы», «Сыбайлас жемқорлыққа қарсы іс-қимыл туралы» заңдары және т.б.;

– ISO/IEC 27001 және ISO/IEC 27002 халықаралық стандарттары;

– 2023–2029 жылдарға арналған Қазақстан Республикасында жоғары білім мен ғылымды дамытудың тұжырымдамасын бекіту туралы;

– Қазақстан Республикасы Ғылым және жоғары білім министрлігінің бұйрықтары мен өкімдері;

– Қоғам қызметінде қолданылатын Қазақстан Республикасының нормативтік-құқықтық актілері мен стандарттары;

– Жоғары білім беру жүйесінің жұмыс істеуі мен дамуын реттейтін өзге де нормативтік-құқықтық актілер.

2.2. Қоғамның ішкі нормативтік құжаттары:

– Қоғамның Жарғысы;

– Корпоративтік басқару кодексі;

– Әдеп кодексі;

– Академиялық адалдық кодексі;

– Академиялық саясат;
– Кадр саясаты;
– Қоғамның даму стратегиялық жоспары.

2. САЯСАТ МАҚСАТЫ

Осы Саясаттың мақсаттары:

– Университеттің құпия ақпаратын сақтау;

– Қызметкерлерді ақпараттық қауіпсіздік мәселелері бойынша оқытуды және олардың хабардарлығын қамтамасыз ету;

– Ақпараттық қауіпсіздік жүйесіне тұрақты түрде тексерулер мен аудиттер жүргізу;

– Университеттің ақпараттық ресурстарының құпиялылығын сақтау;

– Университет контрагенттерімен өзара іс-қимыл барысында кез келген нысанда берілген ақпараттың құпиялылығын сақтау;

– Университеттің іскерлік қызметін қолдау үшін ақпараттық ресурстарға қолжетімділікті қамтамасыз ету;

– Университеттің ақпараттық ресурстарымен байланысты тәуекелдер саласында пайдаланушылардың хабардарлығын арттыру;

– Университетте ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметкерлердің жауапкершілік деңгейі мен міндеттерін айқындау;

– ISO/IEC 27001 және ISO/IEC 27002 халықаралық стандарттарына сәйкес ақпараттық жүйелердің қауіпсіздігін және деректерді қорғауды қамтамасыз ету.

Университет құрылымдық бөлімшелерінің басшылары осы Саясаттың ережелерінің сақталуына тұрақты бақылауды қамтамасыз етуге міндетті. Сонымен қатар, ақпараттық қауіпсіздік талаптарының сақталуына мерзімді түрде тексеру ұйымдастырылып, оның нәтижелері бойынша Университет басшылығына есеп ұсынылуы тиіс.

3. ОСЫ САЯСАТТЫҢ ҚОЛДАНЫЛУ АУҚЫМЫ

4.1. Осы Саясаттың талаптары Университеттің барлық ақпараттарына және ақпаратты өңдеу ресурстарына қолданылады. Осы Саясатты сақтау барлық қызметкерлер үшін (тұрақты және уақытша) міндетті болып табылады.

4.2. Университет ақпаратына қол жеткізетін үшінші тұлғалармен жасалатын шарттарда үшінші тұлғаның осы Саясат талаптарын сақтау міндеті көзделуі тиіс. Үшінші тұлғалармен өзара іс-қимыл жасау барысында ақпаратты жария етпеу туралы келісімге міндетті түрде қол қойылады.

4.3. Университетке меншік құқығымен (оның ішінде зияткерлік меншік құқығымен) Университеттің жалдамалы қызметкерлері әзірлеген барлық бағдарламалық өнімдер, талдамалық деректер, дизайн, сызбалар, сондай-ақ қолданыстағы заңнамаға сәйкес өз қызметін жүзеге асыру мақсатында сатып алынған (алынған) және пайдалануға енгізілген барлық іскерлік ақпарат, лицензиялық бағдарламалық қамтамасыз ету және есептеу ресурстары тиесілі

болып табылады. Аталған меншік құқығы Университет жабдықтарын пайдалана отырып жүзеге асырылатын дауыс және факсимильдік байланысқа, электрондық пошта жәшіктерінің мазмұнына, сондай-ақ Университеттің барлық құрылымдық бөлімшелері мен қызметкерлерінің қағаз және электрондық құжаттарына қолданылады.

5. ТАЛАПТАР МЕН ҰСЫНЫСТАР

5.1. Ақпаратқа қолжетімділікті қамтамасыз етудің жалпы талаптары

Үшінші тұлғаларға Университеттің құпия ақпаратына қолжетімділік беруге тыйым салынады, тек Университет пен дистрибьюторлар мен серіктестер арасындағы тиісті құқықтық құжаттарда (тарату туралы келісімдер немесе басқа серіктестік келісімдер, ақпаратты жарияламау туралы келісімдер) анықталған өзара әрекеттесу жағдайларын қоспағанда, оған деректерді қорғаудың міндетті шарттары және құпия ақпаратты таратуға жауапкершілік кіреді.

5.2. Ақпараттық жүйелерге қолжетімділікті бақылау

Университет кеңселеріндегі барлық жұмыстар тек Университет пайдалануға рұқсат етілген компьютерлерде ғана ресми лауазымдық міндеттерге сәйкес орындалады. Дербес ноутбуктар мен сыртқы сақтау құралдарын (дискілер, флэш-дискілер және т.б.) Университет ғимараттары мен үй-жайларына әкелуге немесе Университеттен алып кетуге болады, тек тікелей басшының келісімімен ғана.

Бөлім басшылары өз қызметкерлерінің және басқа пайдаланушылардың тиісті ақпараттық ресурстарға кіру құқықтарын мезгіл-мезгіл қарап шығуы керек.

Ақпараттық ресурстарға рұқсат етілген кіруді қамтамасыз ету үшін барлық кірулер бірегей пайдаланушы аты мен құпия сөзді пайдаланып орындалуы керек. Қызметкерлер жұмыс орнынан шыққан сайын құпия сөзбен қорғауды орнатуы керек.

5.3. Тіркелгілер және олардың қауіпсіздігі

Пайдаланушылар құпия сөзді таңдағанда және кейіннен пайдаланғанда құпия сөзді қорғау бойынша ұсыныстарды орындауы керек. Үйден жұмыс істеген кезде құпия сөзін басқалармен, соның ішінде отбасы мүшелерімен және жақындарымен бөлісуге немесе беруге қатаң тыйым салынады.

Қызметкерлер ұсынылған құпия сөз күрделілігі талаптарына сай келетін тіркелгілері үшін күрделі құпия сөздер жасауы керек: жеткілікті ұзындықты таңдауы, әртүрлі таңба түрлерін пайдалануы, қарапайым таңбалар тізбегі мен сөздерден аулақ болуы және өздерінің аттарын, тегі мен телефон нөмірлерін пайдаланудан аулақ болуы керек.

Қызметкерлер жұмыс тіркелгілері үшін басқа тіркелгілер, жеке тіркелгілер немесе басқа ұйымдардың тіркелгілері үшін қолданатын құпия сөздерді пайдаланбауы керек.

Қызметкерлер құпия сөздерін үнемі өзгертуі керек. Қауіпсіздікті күшейту үшін Университет пайдаланушылардың құпия сөздерін үнемі өзгертуін қамтамасыз ету үшін құпия сөздің жарамдылық мерзімін бақылау және жарамдылық мерзімін белгілеу әдістерін енгізуі мүмкін.

5.4. Университет жүйелеріне үшінші тараптың қол жеткізуі

Үшінші тұлғалардың Университеттің ақпараттық жүйелеріне қол жеткізуіне тек өндірістік қажеттілік болған жағдайда ғана жол беріледі. Осыған байланысты Университеттің ақпараттық ресурстарына қол жеткізу Университет басшылығының рұқсаты негізінде жүзеге асырылады.

5.5. Қашықтан қол жеткізу

Қызметкерлерге өздерінің лауазымдық міндеттеріне негізделген Университеттің ақпараттық ресурстарына қашықтан қол жеткізу құқығы беріледі. Қол жеткізуді беру үшін олар қажеттілікті негіздеп, қол жеткізуге өтініш беруі керек.

Университеттің жұмыс компьютерлеріне қол жеткізуді қажет ететін қызметкерлерге осы жұмыс станцияларына қашықтан қол жеткізу берілуі мүмкін, олар корпоративтік ақпараттық жүйедегі құқықтарына сәйкес жұмысты орындай алады және Университеттің желілік ресурстарына қол жеткізе алады.

Университетке тиесілі емес компьютерді пайдаланып, Университеттен тыс жерде жұмыс істейтін қызметкерлерге қашықтан қол жеткізетін компьютерге деректерді көшіруге тыйым салынады. Университеттің ақпараттық ресурстарына қашықтан қол жеткізуге уәкілетті қызметкерлер мен үшінші тараптар өз компьютерлерінің Университет желісіне және Университетке тиесілі емес кез келген басқа желілерге бір уақытта қосылмауы туралы талапты сақтауы керек.

Сыртқы желілерден Университеттің ақпараттық желісіне қашықтан қол жеткізу арқылы қосылған барлық компьютерлерде жаңартылған антивирустық бағдарламалық жасақтама болуы керек.

Техникалық құралдар операциялық жүйені немесе бағдарламалық жасақтаманы жаңарту талаптарына, вирус жазбаларына немесе антивирустық бағдарламалық жасақтамаға қойылатын талаптарға сай келмейтін немесе қорғанысы жоқ компьютерлер үшін Университет желілері мен ресурстарына кіруді шектеу үшін пайдаланылуы мүмкін.

Қашықтан кіру бағдарламалық жасақтамасын орнатуға, іске қосуға немесе пайдалануға тыйым салынады. Ақпараттық жүйелер және техникалық қолдау қызметкерлеріне арналған қашықтан қосылу бағдарламалық шешімдері тек Университеттің ішкі желісінде ғана пайдаланылуы мүмкін. Қашықтан көмек көрсету үшін қызметкерлер Университетте пайдалануға рұқсат етілген корпоративтік коммуникаторлар ұсынатын басқарылатын қашықтан қосылуларды немесе экранды ортақ пайдалану мүмкіндіктерін пайдалана алады.

5.6. Интернетке қолжетімділік

Интернетке қолжетімділік тек іскерлік мақсаттар үшін беріледі және заңсыз әрекеттер үшін пайдаланылмауы тиіс. Университет қызметкерлеріне интернетті тек ресми мақсаттарда пайдалануға рұқсат етіледі.

Қоғамдық пікірге қорлайтын немесе жыныстық қатынасқа қатысты ақпарат, нәсілдік жеккөрушілікті насихаттау, гендерлік айырмашылықтар/артықшылықтар туралы пікірлер, жала жабу туралы мәлімдемелер немесе біреудің жасына,

жыныстық бағдарына, діни немесе саяси сенімдеріне, ұлттық тегіне немесе мүгедектігіне қатысты қорлайтын сөздері бар басқа материалдар бар кез келген веб-сайтқа кіруге тыйым салынады. Экстремистік немесе террористік сипаттағы ресурстарға, порнографиялық мазмұнға немесе Қазақстан Республикасының заңнамасымен тыйым салынған мазмұнға кіруге тыйым салынады.

Жеке немесе басқа ұйымдардың есептік жазбаларын пайдаланып, ресми немесе корпоративтік ақпаратты сақтау үшін бұлттық ресурстарды пайдалануға тыйым салынады. Бұл ақпаратты сақтауға, жіберуге және синхрондауға тек Университет ұсынған корпоративтік есептік жазбаларды пайдаланатын корпоративтік және жұмыс мақсаттары үшін бекітілген бұлттық қызметтерде ғана рұқсат етіледі. Университет корпоративтік қызметтер тізіміне кірмейтін бұлттық қызметтерді бұғаттауы мүмкін.

Мемлекеттік провайдерлер ұсынған жеке есептік жазбалары бар қызметкерлерге оларды Университетке тиесілі жабдықта пайдалануға рұқсат етілмейді.

Университет қызметкерлері интернет арқылы алынған файлдарды ашпас немесе таратпас бұрын оларды вирустарға сканерлеуі керек.

Университет интернет байланысы арқылы екі бағытта да ағып жатқан барлық ақпараттың мазмұнын бақылау құқығын өзінде қалдырады. Сондай-ақ, ресурстарға қолмен немесе автоматтандырылған алгоритмдер, аппараттық құралдар, бағдарламалық жасақтама, желілік және ақпараттық қауіпсіздік жүйелері арқылы қол жеткізуді шектеуі мүмкін.

5.7. Жабдық қауіпсіздігі

Қызметкерлер Университет ақпаратын сақтайтын жабдықтың физикалық қауіпсіздігін қамтамасыз ету қажеттілігін әрқашан есте ұстауы керек.

Қызметкерлерге аппараттық және бағдарламалық жасақтама конфигурациясын өз бетінше өзгертуге тыйым салынады. Барлық өзгерістерді тек жүйелік әкімшілер және техникалық қолдау мамандары енгізуі тиіс.

5.8. Аппараттық құрал

Барлық компьютерлік жабдықтар (серверлер, үстел үсті және ноутбук компьютерлері), деректерді сақтау жабдықтары (жад карталары, портативті қатты дискілер, CD-ROM дискілері), перифериялық құрылғылар (мысалы, мониторлар, принтерлер және сканерлер), керек-жарақтар (көрсеткіш құрылғылар, енгізу құрылғылары, CD-ROM дискілері) және байланыс жабдықтары (мысалы, желілік адаптерлер мен хабтар) осы Саясаттың мақсаттары үшін бірге «компьютерлік жабдық» деп аталады. Компания ұсынатын компьютерлік жабдық оның меншігі болып табылады және тек іскерлік мақсаттарда пайдалануға арналған. Құпия деп белгіленген және Университеттің коммерциялық құпиясын құрайтын ақпараты бар портативті компьютерлерді пайдаланушылар компьютер пайдаланылмаған кезде олардың физикалық тұрғыдан қауіпсіз жерлерде, құлыпталған үстел тартпаларында, шкафтарда немесе бірдей тиімді қорғаныс құралымен қорғалуын қамтамасыз етуі тиіс.

Ноутбук алған әрбір қызметкер оның кеңседе де, үйде де қауіпсіздігін қамтамасыз ету үшін тиісті шараларды қабылдауға жауапты. Ноутбук ұрлану қаупі артатын жағдайларда, мысалы, қонақ үйлерде, әуежайларда, іскерлік серіктестердің кеңселерінде және т.б., пайдаланушылар ноутбуктарын ешқашан қараусыз қалдырмауы керек.

Жүйені іске қосу, жылдам пернелерді іске қосу және экран сақтағыш режимінен шыққаннан кейін барлық компьютерлер құпия сөзбен қорғалуы керек. Жабдықтың жоғалуына әкеп соқтыратын абайсыздық немесе немқұрайлылық салдарынан деректерге қол сұғылмауы керек. Жою алдында сақтау құралдарын (қатты дискілерді қоса алғанда) қамтитын жабдықтың барлық компоненттері құпия деректер немесе лицензияланған өнімдер жоқ екеніне көз жеткізу үшін тексерілуі керек. Сақтау құралдары деректерді қалпына келтірудің алдын алу үшін пішімделуі керек.

Кез келген ақпаратты тұтынушыларға немесе іскерлік серіктестерге тарату үшін сақтау құралдарына жазған кезде, ақпараттың таза екеніне және басқа деректер жоқ екеніне көз жеткізіңіз. Сақтау құрылғысын қайта пішімдеу онда сақталған ақпараттың толық жойылуына кепілдік бермейді. Смартфондар сенімді деректерді қорғау механизмдері бар құрылғылар емес. Мұндай құрылғыда құпия ақпаратты сақтау ұсынылмайды.

5.9. Ақпараттық қауіпсіздік шараларының мысалдары

Ұйым өз жүйелері мен деректерінің ақпараттық қауіпсіздігін қамтамасыз ету үшін келесі шараларды қолдана алады:

Техникалық шаралар – мысалы, рұқсатсыз кірудің алдын алу үшін қауіпсіздік құралдарын пайдалану, деректерді шифрлау және сақтық көшірмелеу.

Ұйымдастыру шаралары – мысалы, қызметкерлерді ақпараттық қауіпсіздік бойынша оқыту, ақпараттық қауіпсіздік саясатын жасау және ақпараттық қауіпсіздік бойынша тұрақты аудиттер жүргізу.

Әкімшілік шаралар – мысалы, жүйелер мен деректерге кіруді басқару және ақпараттық жүйелерді пайдалануды бақылау.

5.10. Қауіптер мен осалдықтарға шолу

Ақпараттық жүйе әртүрлі қауіптер мен осалдықтарға ұшырауы мүмкін. Ең көп таралған қауіптерге мыналар жатады:

- Рұқсатсыз кіру - Ақпаратқа немесе жүйеге рұқсатсыз кіру
- Пайдалану - Ақпаратты немесе жүйені рұқсатсыз пайдалану
- Ашу - Ақпаратты немесе жүйені рұқсатсыз тарату
- Өзгерту - Ақпаратты немесе жүйені рұқсатсыз өзгерту
- Жою - Ақпаратты немесе жүйені рұқсатсыз жою
- Ең көп таралған осалдықтарға мыналар жатады:
- Бағдарламалық жасақтама қателері - Бағдарламалық жасақтамадағы қателерді шабуылдаушылар жүйеге немесе ақпаратқа кіру үшін пайдалана алады

– Қауіпсіз емес конфигурациялар - Қауіпсіз емес жүйе конфигурациялары жүйені шабуылға осал етуі мүмкін

– Инфрақұрылымның әлсіз жақтары - Жүйе инфрақұрылымындағы әлсіздіктер, мысалы, әлсіз құпия сөздер немесе сақтық көшірмелердің болмауы, оны шабуылға осал етуі мүмкін.

5.11. Жаңартулар

Бағдарламалық жасақтама мен аппараттық құралдарды жаңарту ақпараттық қауіпсіздікті қамтамасыз етудегі маңызды фактор болып табылады. Жаңартулар шабуылдаушылар жүйеге немесе ақпаратқа қол жеткізу үшін пайдалана алатын қателерді түзетуді қамтуы мүмкін. Жаңартулар сонымен қатар жүйе қауіпсіздігін жақсарта алатын жаңа мүмкіндіктерді қамтуы мүмкін.

Жаңартулардың түрлері:

– Қателерді түзету - бағдарламалық жасақтамадағы немесе аппараттық құралдардағы қателерді түзететін жаңартулар.

– Осалдық патчтары - бағдарламалық жасақтамадағы немесе аппараттық құралдардағы осалдықтарды түзететін жаңартулар.

– Функция патчтары - бағдарламалық жасақтамаға немесе аппараттық құралдарға жаңа мүмкіндіктер қосатын жаңартулар.

Жаңартулардың маңыздылығы:

Жаңартулар қателерді түзету және осалдықтарды жою арқылы жүйе қауіпсіздігін жақсарта алады.

– Жаңартулар жүйе қауіпсіздігін жақсарта алатын жаңа мүмкіндіктерді қоса алады.

– Жаңартуларды орнатпау жүйені зиянды шабуылдарға осал етеді.

– Жаңартуларды басқарудың ең жақсы тәжірибелері:

– Ұйымда жаңартуларды орнату тәртібі мен уақытын анықтайтын жаңартуларды басқару саясаты болуы керек.

– Ұйым қызметкерлердің жаңартуларды орнатудың маңыздылығын білуін қамтамасыз етуі керек.

Жаңартулардың мысалдары:

– Бағдарламалық жасақтама жаңартулары – қателерді түзету, қауіпсіздік жаңартулары және операциялық жүйелер, қолданбалар және веб-шолғыштар сияқты бағдарламалық жасақтамаға арналған жаңа мүмкіндіктер. Аппараттық құрал жаңартулары – желілік жабдықтар, серверлер және жұмыс станциялары сияқты аппараттық құралдарға арналған қателерді түзету және қауіпсіздік жаңартулары.

5.12. Бағдарламалық жасақтама

Компания ұсынған компьютерлік жабдыққа орнатылған барлық бағдарламалық жасақтама Университеттің меншігі болып табылады және тек өндірістік мақсаттарда пайдаланылуы тиіс.

Қызметкерлерге пайдалануға берілген компьютерлік жабдыққа стандартты емес, лицензияланбаған бағдарламалық жасақтаманы немесе олардың жұмысына қатысы жоқ бағдарламалық жасақтаманы орнатуға тыйым салынады. Техникалық қызмет көрсету кезінде рұқсат етілмеген бағдарламалық жасақтама анықталған жағдайда, ол жойылады және бұзушылық туралы есеп қызметкердің тікелей басшысына жіберіледі.

Барлық компьютерлер ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті бағдарламалық жасақтамамен, соның ішінде антивирустық бағдарламалық жасақтамамен және жеке брандмауэрмен жабдықталуы тиіс.

Университет қызметкерлеріне:

– антивирустық бағдарламалық жасақтаманы блоктауға;

– басқа антивирустық бағдарламалық жасақтаманы орнатуға;

– антивирустық бағдарламалық жасақтаманың параметрлері мен конфигурациясын өзгертуге тыйым салынады.

Корпоративтік жүйелерге бағдарламалық жасақтаманы орнатуға шектеу шаралары қолданылады. Қажетті бағдарламалық жасақтаманы корпоративтік құрылғыларға орнату үшін қызметкерлер қажетті бағдарламалық жасақтаманы орнату үшін Техникалық қолдау бөліміне хабарласуы керек. Орнату қажеттілігі негізделіп, лицензияланған болуы керек немесе бағдарламалық жасақтама еркін пайдаланылуы және тегін лицензиясы болуы керек.

5.13. Электрондық поштаны пайдаланудың ұсынылатын ережелері

Электрондық пошта хабарламаларының мазмұны корпоративтік іскерлік этика стандарттарына қатаң сәйкес келуі керек.

Электрондық поштаны жеке пайдалануға хабарламаларды алу/жіберу басқа пайдаланушылардың жұмысына немесе іскерлік қызметке кедергі келтірмеген жағдайда рұқсат етіледі. Университеттің құпия ақпаратын ешқандай жағдайда электрондық пошта арқылы үшінші тараптарға жіберуге болмайды.

Университет қызметкерлеріне кез келген корпоративтік қызмет үшін қоғамдық, жеке немесе басқа ұйымдардың электрондық пошта тіркелгілерін пайдалануға тыйым салынады. Университет қоғамдық электрондық пошта қызметтеріне қол жеткізуге шектеулер қоюы мүмкін. Университет қызметкерлерінің қоғамдық электрондық пошта тіркелгілерін пайдалануына тек Университет басшылығының келісімімен рұқсат етіледі.

Университет қызметкерлері іскерлік серіктестермен құжаттар алмасқан кезде тек ресми электрондық пошта мекенжайын пайдалануы керек.

Электрондық пошта хабарламалары электрондық байланыс үшін үнемі қолданылатын құрал болып табылады, хаттар мен факстармен бірдей мәртебеге ие. Электрондық хабарламалар басқа жазбаша хабарламалар сияқты бекіту және сақтау талаптарына бағынады.

Хабарламаларды жіберу кезінде қателіктердің алдын алу үшін пайдаланушылар жіберу алдында алушылардың аты-жөндері мен мекенжайларының емлесін мұқият тексеруі керек. Егер хабарлама арналмаған

біреуге келіп түссе, ол тікелей алушыға жіберілуі керек. Егер осылайша алынған ақпарат құпия болса, бұл туралы тікелей басшыға дереу хабарлау қажет.

Электрондық хабарламаны немесе құжатты жіберуші немесе оны жіберген адам өзінің аты-жөнін, жұмыс мекенжайын және хабарламаның тақырыбын көрсетуі тиіс.

Электрондық поштаны пайдалануға тыйым салынған әрекеттер мен жағдайлар:

– маңызды электрондық пошта ресурстарын пайдаланатын жеке хабарламаларды жіберу;

– Университеттің барлық пайдаланушыларына топтық хабарламалар/электрондық пошталар жіберу;

– Университеттің қызметіне қатысы жоқ жарнамалық материалдарды жіберу;

– пошта тізімдеріне жазылу, талқылауларға қатысу және жеке мақсаттар үшін маңызды электрондық пошта ресурстарын пайдаланатын ұқсас қызметтер;

– басқаларға жіберілген хабарламаларды іздеу және оқу (олардың қалай сақталғанына қарамастан);

– Заңсыз, әдепсіз, зиянды, қорлайтын, қорқытатын, жала жабатын, зиянды немесе қылмыстық құқық бұзушылық немесе құқық бұзушылық деп саналуы мүмкін немесе азаматтық жауапкершілікке, тәртіпсіздіктерге әкеп соқтыратын немесе корпоративтік этикалық стандарттарға қайшы келетін кез келген материалдарды, хабарламаларды немесе қосымшаларды жіберу.

Пайдаланушы сыртқы пайдаланушыларға жіберілген барлық шығыс хабарламаларға құпиялылық туралы ескерту қоса алады.

Бір хабарламада айтарлықтай көлемдегі деректерді жіберу қызметкердің кіріс жәшігінің қолжетімділігіне кері әсер етуі мүмкін. Бір хабарламадағы тіркемелердің өлшемі 25 МБ-тан аспауы керек.

5.14. Корпоративтік коммуникациялар

Қызметкерлердің жедел байланысы үшін корпоративтік мессенджерлерді жұмыс компьютерлерінде де, жеке мобильді құрылғыларда да пайдалану қажет. Мобильді құрылғылар рұқсатсыз кіруден қорғалуы керек. Кіруді қорғау әдістері құрылғыны құпия сөзбен, PIN-кодпен, пайдаланушы биометриясымен немесе басқа қауіпсіздік әдістерімен қорғауды қамтамасыз етуі керек. Кез келген корпоративтік мәселелер үшін жеке тіркелгілері бар мессенджерлерді пайдалануға тыйым салынады. Құжаттарды сыртқы немесе дұрыс емес алушыларға кездейсоқ жіберу салдарынан ақпараттың ағып кетуіне жол бермеу үшін ішкі құжаттарды, олардың сканерленген көшірмелерін немесе мөрлер мен қолтаңбалары бар фотосуреттерді жіберуге қатаң тыйым салынады.

5.15. Ақпараттық қауіпсіздік оқиғалары туралы хабарлау, оларға жауап беру және хабарлау

Барлық пайдаланушыларға тікелей басшысы ақпараттық қауіпсіздіктің белгілі немесе күдікті бұзушылықтары туралы хабарлау міндеттемесі туралы хабарлауы керек және кез келген жағдайда білетін қауіпсіздік әлсіздіктерін пайдалануға тырыспау туралы нұсқау берілуі керек.

Компьютер ұрланған жағдайда, оқиға туралы дереу тікелей басшысына хабарлау керек.

Егер вирустар немесе басқа да деструктивті компьютерлік код күдіктенсе немесе анықталса, қызметкерлер мыналарды орындауы керек:

– қолдау мамандарына хабарлау;

– зарарланған компьютерді пайдаланбау немесе өшірмеу;

– Анықталған вирус жойылғанша және қолдау мамандары толық антивирустық сканерлеу жүргізгенше компьютерді университеттің компьютерлік желісіне қоспаңыз.

5.16. Ақпараттық қауіпсіздік жабдықтары бар бөлмелер

Құпия кездесулер (сессиялар) тек ақпараттық қауіпсіздік жабдықтарымен қорғалатын бөлмелерде өткізілуі тиіс.

Ақпараттық қауіпсіздік жабдықтары бар бөлмелердің тізімін Университет әкімшілігі бекітеді.

Құпия кездесулер кезінде аудио/бейнежазба және фотосуретке түсіруді тек кездесудің топ жетекшісінің жазбаша рұқсатын алғаннан кейін кездесуді дайындауға жауапты Университет қызметкері ғана жүргізе алады.

5.17. Желіні басқару

Университет қызметкерлеріне мыналарға тыйым салынады:

– ақпараттық қауіпсіздікті және Университет желісінің жұмысын бұзуға; порттарды немесе қауіпсіздік жүйесін сканерлеуге;

– деректерді ұстап алу арқылы желінің жұмысын бақылауға;

– пайдаланушыны сәйкестендіру немесе қауіпсіздік жүйесін айналып өтіп, компьютерге, желіге немесе тіркелгіге кіруге;

– соңғы нүкте құрылғысының пайдаланушысына кедергі келтіру немесе оны ажырату мақсатында кез келген бағдарламаларды, сценарийлерді, командаларды пайдалануға немесе хабарламаларды жіберуге;

– Университет қызметкерлері туралы ақпаратты немесе Университет қызметкерлерінің тізімдерін рұқсатсыз тұлғаларға беруге;

– компьютерлік вирустарды және басқа да деструктивті бағдарламалық жасақтаманы жасауға, жаңартуға немесе таратуға.

5.18. Деректерді қорғау және қауіпсіздік

Пайдаланушылар үстел үсті және ноутбук компьютерлеріндегі деректердің қауіпсіздігіне жауапты.

Барлық маңызды қызметтік деректер мен бағдарламалық жасақтаманың сақтық көшірмелерін үнемі жасау қажет. Барлық қызметтік ақпаратты корпоративтік тіркелгінің бұлттық сақтау орнымен синхрондауға

конфигурацияланған жұмыс станциясының қалталарында сақтау ұсынылады, бұл сақтық көшірмелерді және құжаттардың нұсқасын қамтамасыз етеді. Егер синхрондау қосылмаған болса, деректерді корпоративтік тіркелгінің бұлттық сақтау орнының веб-интерфейсі арқылы сақтауға болады.

Қызметкерлер ортақ желілік ресурстарда файлдар мен каталогтарды тек оларға жеке, жұмыс топтарына бөлінген немесе рұқсат етілген кіру мүмкіндігі бар аймақтарда ғана жасай, өзгерте және жоя алады.

5.19. Ақпараттың құпиялылығы

Ақпараттың құпиялылығы дегеніміз, ақпарат тек ол кімге арналған болса, соларға ғана қолжетімді. Құпиялылық ақпараттық қауіпсіздіктің негізгі аспектілерінің бірі болып табылады.

Ақпараттың құпиялылығын қамтамасыз ету үшін ұйым келесі шараларды қолдана алады:

– Ақпаратты рұқсатсыз кіруден қорғау үшін шифрлауды қолданыңыз. Деректерді шифрлау ақпаратты бұзушылар үшін қолжетімсіз етеді, тіпті олар ақпараттық қауіпсіздік пен университет желісіне қауіп төндіру арқылы оған қол жеткізсе де; сканерлеу порттары немесе қауіпсіздік жүйесі;

– Ақпаратқа қол жеткізуді уәкілетті тұлғалармен шектеу. Ұйымда кімнің қандай ақпаратқа қол жеткізе алатынын анықтайтын ақпаратқа қол жеткізуді бақылау саясаты болуы керек.

– Енді қажет емес ақпаратты дұрыс жою. Енді қажет емес ақпарат оны қалпына келтіру мүмкін еместігіне көз жеткізетіндей етіп жойылуы керек.

Ақпараттың құпиялылығын қамтамасыз ету шараларының мысалдары:

– Желі арқылы берілетін деректерді қорғау үшін шифрлауды пайдалану.

– Сақтау құралдарында сақталған деректерді қорғау үшін шифрлауды пайдалану.

– Ақпаратқа қол жеткізуді уәкілетті тұлғалармен шектеу үшін ақпаратқа қол жеткізу саясатын пайдалану.

– Ақпаратқа тек уәкілетті құрылғылардан қол жеткізуді қамтамасыз ету үшін қашықтан қол жеткізу құралдарын пайдалану.

– Ескірген немесе қажетсіз ақпаратты үнемі жою.

5.20. Тәуекелдерді басқару процестері

Тәуекелдерді басқарудың негізгі процестері:

– Анықтау — ақпараттық қауіпсіздіктің ықтимал тәуекелдерін анықтау.

– Бағалау — тәуекелдердің ықтималдығы мен салдарын анықтау.

– Басқару — тәуекелдерді азайту шараларын енгізу.

– Мониторинг — тәуекелдерді азайту шараларының тиімділігін бақылау.

– Жоспарлау — тәуекелдерді басқару мақсаттары мен міндеттерін анықтау және іс-қимыл жоспарын әзірлеу.

5. ЖОСПАРЛАУ

Жоспарлау кезеңінде ұйым тәуекелдерді басқару мақсаттары мен міндеттерін анықтайды және іс-қимыл жоспарын әзірлейді.

Негізгі жоспарлау міндеттеріне мыналар кіреді:

– Тәуекелдерді басқаруға қатысушылардың құрамы мен міндеттерін анықтау.

– Тәуекелдерді басқару әдіснамасын әзірлеу.

– Тәуекелдерді басқару мақсаттары мен міндеттерін анықтау.

– Тәуекелдерді бағалау үшін ақпарат көздерін анықтау.

6. ИДЕНТИФИКАЦИЯЛАУ

Идентификациялау кезеңінде ұйым ақпараттық қауіпсіздіктің ықтимал тәуекелдерін анықтайды. Тәуекелдерді анықтаудың негізгі әдістеріне мыналар жатады:

– Ақпараттық қауіпсіздік оқиғаларын талдау

– Реттеуші талаптарды талдау

– Ұйымдастырушылық қызметті талдау

– Қауіптер мен осалдықтарды талдау, тәуекелдерді басқару мақсаттары мен міндеттерін анықтау

6.1. Бағалау

Бағалау кезеңінде ұйым тәуекелдердің ықтималдығы мен салдарын анықтайды.

Тәуекелдерді бағалаудың негізгі әдістеріне мыналар жатады:

– Сандық тәуекелді бағалау

– Сапалық тәуекелді бағалау

6.2. Басқару

Басқару кезеңінде ұйым тәуекелдерді азайту үшін шаралар қабылдайды.

Тәуекелдерді басқарудың негізгі әдістеріне мыналар жатады:

– Тәуекелдерді жою

– Тәуекелдердің ықтималдығын азайту

– Тәуекелдердің салдарын азайту

6.3. Мониторинг

Мониторинг кезеңінде ұйым тәуекелдерді азайту шараларының тиімділігін бақылайды.

Мониторингтің негізгі әдістеріне мыналар жатады:

– Тәуекелдерді азайту туралы есептерді талдау

– Тұрақты тәуекелді бағалау

– Ақпараттық қауіпсіздік оқиғаларын талдау

7. АҚПАРАТТЫҢ ТҰТАСТЫҒЫ

Ақпараттың тұтастығы ақпараттың рұқсатсыз өзгертілмегенін білдіреді. Тұтастық ақпараттық қауіпсіздіктің негізгі аспектісі болып табылады.

Ақпараттың тұтастығын қамтамасыз ету үшін ұйым келесі шараларды қолдана алады:

– Ақпараттағы өзгерістерді анықтау үшін тұтастықты бақылау құралдарын пайдаланыңыз. Тұтастықты бақылау құралдары ақпараттың рұқсатсыз өзгертілгенін анықтауға көмектеседі.

– Өзгерту немесе жою жағдайында қалпына келтіру үшін деректерді үнемі сақтық көшірмелеу. Сақтық көшірмелер өзгерту немесе жою жағдайында ақпаратты қалпына келтіруге мүмкіндік береді.

Ақпараттың тұтастығы шараларының мысалдары:

– Файлдар мен дерекқорлар үшін тұтастықты бақылау құралдарын пайдаланыңыз.

– Деректердің үнемі сақтық көшірмесін жасаңыз.

– Деректерді рұқсатсыз өзгертуден қорғау үшін шифрлауды пайдаланыңыз.

– Деректерге рұқсатсыз өзгертулерді шектеу үшін ақпаратқа қол жеткізу саясатын пайдаланыңыз.

Ақпараттың тұтастығын қамтамасыз ету бойынша ұсыныстар:

– Тұтастық тәуекелдерін бағалаңыз. Ұйым ақпараттың тұтастығын бұзу тәуекелдерін бағалап, бұл тәуекелдерді азайту шараларын әзірлеуі керек.

– Қызметкерлерді оқыту. Ұйым қызметкерлері ақпараттың тұтастығының маңыздылығын және оны қалай қорғау керектігін білуі керек.

Ақпараттың тұтастығы оқиғаларының мысалдары:

– Ақпаратты рұқсатсыз өзгерту.

– Ақпараттың жойылуы немесе зақымдануы.

Ақпараттың тұтастығына әсер ету оқиғалары:

– Қаржылық шығындар

– Беделдің жоғалуы

– Заңнаманы бұзу

Құпиялылық пен тұтастықты салыстыру:

Құпиялылық пен тұтастық ақпараттық қауіпсіздіктің екі негізгі аспектісі болып табылады. Құпиялылық дегеніміз ақпарат тек ол кімге арналған болса, соларға ғана қолжетімді екенін білдіреді. Тұтастық дегеніміз ақпараттың рұқсатсыз өзгертілмегенін білдіреді.

8. АҚПАРАТТЫҢ ҚОЛЖЕТІМДІЛІГІ

Ақпараттың қолжетімділігі ақпараттың қажетті уақытта және орында мақсатты пайдалану үшін қолжетімді болуын білдіреді. Қолжетімділік ақпараттық қауіпсіздіктің негізгі аспектісі болып табылады.

Ақпараттың қолжетімділігін қамтамасыз ету үшін ұйым келесі шараларды қолдана алады:

– Жүйе істен шыққан жағдайда ақпаратқа қол жеткізуді қамтамасыз ету үшін резервтік көшірмелерді пайдаланыңыз. Резервтік көшірмелер ақпараттың жоғалуы немесе бүлінуі жағдайында оны қалпына келтіруге мүмкіндік береді.

– Бизнестің үздіксіздігін қамтамасыз ету үшін жүйелерді бірнеше географиялық орталықтарда орналастырыңыз. Жүйелерді бірнеше орталықта орналастыру бір орталықта істен шыққан жағдайда да ақпаратқа қол жеткізуді қамтамасыз етеді.

– Ақауларды жедел анықтау және шешу үшін бақылау және ескерту құралдарын пайдаланыңыз. Бақылау және ескерту ақауларды уақтылы анықтауға және түзету шараларын енгізуге мүмкіндік береді.

Ақпараттың қолжетімділігін қамтамасыз ету шараларының мысалдары:

– Файлдар мен дерекқорлар үшін резервтік көшірмелерді пайдаланыңыз.

– Жүйелерді бірнеше деректер орталықтарында орналастырыңыз.

– Жүйелер мен желілер үшін бақылау және ескерту құралдарын пайдаланыңыз.

– Жүйелер мен желілер үшін ақауға төзімді компоненттерді пайдаланыңыз.

Ақпараттың қолжетімділігі бойынша ұсыныстар:

– Қолжетімділік тәуекелін бағалау. Ұйым ақпаратқа қолжетімділіктің бұзылуы тәуекелдерін бағалауы және осы тәуекелдерді азайту шараларын әзірлеуі тиіс.

– Қызметкерлерді оқыту. Ұйым қызметкерлері ақпаратқа қолжетімділіктің маңыздылығын және оны қалай қамтамасыз ету керектігін білуі керек.

– Үнемі мониторинг және аудит жүргізу. Ұйым ақпаратқа қолжетімділік шараларының тиімділігін үнемі бақылауы керек.

Ақпаратқа қолжетімділік оқиғаларының мысалдары:

– Жүйенің немесе желінің істен шығуы.

– Жүйелердің немесе желілердің жойылуы немесе зақымдануы.

– Кибершабуыл.

– Ақпаратқа қолжетімділік оқиғаларының әсері:

– Қаржылық шығындар.

– Беделдің жоғалуы.

– Заңнаманы бұзу.

КЕЛІСУ ПАРАҒЫ

№	Қызметі	Т.А.Ә	Күні	Қолы
1	Басқарма Мүшесі – Аппарат басшысы	Сугирбекова К.С.		
2	HR департаментінің директоры	Маликова А.А.		
3	Заң қызметінің басшысы	Ильясов Р.М.		
4	Сапа менеджменті жүйесі бөлімінің басшысы	Тауасарова А.С.		

ТАНЫСУ ПАРАҒЫ

№	Т.А.Ә.	Қызметі	Күні	Қолы	Ескертпе

ӨЗГЕРІСТЕРДІ ТІРКЕУ ПАРАҒЫ

№ өзгеріс	Өзгерістер енгізілуге жататын бөлім, тармақ	Өзгеріс түрі (ауыстыру, күшін жою, толықтыру)	Өзгерістер енгізудің негіздемесі	Өзгеріс енгізілді		
				Күні	Т.А.Ә	Қолы