«Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КеАҚ

BU
BAITURSYNULY UNIVERSITY

Бекітемін
Басқарма Төрағасы - Ректор
_____ С.Куанышбаев
_____ 2024 ж.

САЯСАТ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК
«АХМЕТ БАЙТҰРСЫНҰЛЫ
АТЫНДАҒЫ ҚОСТАНАЙ ӨҢІРЛІК УНИВЕРСИТЕТІ» КЕАҚ

С 054-2024

Қостанай

Алғы сөз

1 Бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімімен
ӘЗІРЛЕНДІ

2 Бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімімен
ЕНГІЗІЛДІ

3 Қоғам Басқармасының 17.07.2024 жылғы № 08 хаттама шешімімен
БЕКІТІЛДІ ЖӘНЕ ҚОЛДАНЫСҚА ЕНГІЗІЛДІ

4 ӘЗІРЛЕУШІ:
В. Гриднева – бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімі бастығы;

5 САРАПШЫЛАР:
А.Шмит – техникалық қамтамасыз ету бөлімінің бастығы

6 ТЕКСЕРУ МЕРЗІМДІЛІГІ 3 жыл

7 Алғаш рет **ЕНГІЗІЛДІ**

Мазмұны

1 Тарау. Жалпы ережелер мен қолдану аясы

1. Бұл Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университетінің АҚ (бұдан әрі – Университет) Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университетінің АҚ (бұдан әрі – Университет) ақпараттық қауіпсіздігін қамтамасыз ету саласындағы мақсаттарды, міндеттерді, басты принциптерді және тәжірибелік әдістерді айқындайды.

2. Бұл Саясатта ақпараттық қауіпсіздік деп Университеттің электрондық ақпараттық ресурстарының, ақпараттық жүйелерінің және деректер базаларының сыртқы және ішкі қауіптерден қорғалғандығы түсіндіріледі. Бұл Университетке материалдық шығын келтіруі мүмкін, беделіне зиян келтіруі мүмкін немесе Университеттің қызметкерлері мен оқытушыларына басқа да зиян келтіруі мүмкін қауіптер.

3. Саясат Университеттің нормативтік-анықтамалық құжаттамасының құрамына кіреді және Университеттің барлық қызметкерлері үшін міндетті орындалуы тиіс. Сонымен қатар, ол Университеттің ақпараттық жүйелері мен құжаттарына қол жеткізетін үшінші тұлғаларға да хабарланады.

2 Тарау. Нормативтік сілтемелер

4. Саясат мынадай құжаттардың талаптары мен ұсыныстарына сәйкес әзірленген және процедураларды белгілейді:

1) «Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы;

2) «Ақпаратқа қол жеткізу туралы» Қазақстан Республикасының 2015 жылғы 16 қарашадағы № 401-V Заңы;

3) «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 Қаулысы;

4) ҚР СТ ISO/IEC 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар»;

5) ҚР СТ ISO/IEC 27005-2022 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік тәуекелі менеджменті»;

6) Қазақстан Республикасы Қаржы министрлігі Мемлекеттік мүлік және жекешелендіру комитеті Төрағасының 2020 жылғы 05 маусымдағы № 350 бұйрығымен бекітілген «А.Байтұрсынов атындағы Қостанай өңірлік университеті» КЕАҚ Жарғысы;

7) ҰС 081-2022. Ұйым стандарты. Іс қағаздарын жүргізу;

8) ҚП 082-2022. Құжаттау процедурасы. Құжаттаманы басқару.

3 Тарау. Белгілер мен қысқартулар

5. Осы Ережеде мынадай терминдер мен анықтамалар қолданылады:
1. АҚ – Ақпараттық қауіпсіздік;
2. БҚ – Бағдарламалық қамтамасыз ету;
3. АЖ – Ақпараттық жүйе;
4. АҚБЖ – Ақпараттық қауіпсіздікті басқару жүйесі.

4 Тарау. АҚ негізгі мақсаттары мен міндеттері

6. Бұл Саясат Университеттің электрондық ақпараттық ресурстарын, ақпараттық жүйелерін және деректер базаларын рұқсатсыз қол жеткізу, пайдалану, ашу, бұрмалау, өзгерту немесе жоюдан қорғауға бағытталған ұйымдастырушылық және техникалық шаралардың кешенін іске асыру мақсатында әзірленген.

7. Университетте ақпараттық қауіпсіздіктің міндеттері ақпаратты және желілік инфрақұрылымды қорғауды қамтамасыз етуге бағытталған кең спектрлі шараларды және әрекеттерді қамтиды:

1) Деректердің құпиялылығын қорғау: Университеттің электрондық ақпараттық ресурстарын, ақпараттық жүйелерін, деректер базаларын, қызметкерлердің, оқытушылардың жеке деректерін, қаржылық ақпаратты, зерттеулерді және басқа да құпия деректерді заңсыз әрекеттерден, ықтимал қауіптерден, рұқсатсыз қол жеткізуден, ағудан немесе ұрлаудан қорғау. Университеттің тұтынушылары мен серіктестерімен өзара әрекеттесу процесінде кез келген түрде берілген ақпараттың құпиялылығын сақтау.

2) Деректердің тұтастығын қамтамасыз ету: Университеттің электрондық ақпараттық ресурстарының, ақпараттық жүйелерінің және деректер базаларының тұтастығын қамтамасыз ету, рұқсатсыз өзгертулерден немесе зақымданулардан сақтау.

3) Деректерге қол жеткізуді қамтамасыз ету: Университеттің ақпараттық жүйелеріне рұқсат берілген пайдаланушылар үшін оқу және әкімшілік процестерінің үздіксіздігін қамтамасыз ету үшін қажетті көлемде қол жеткізуді қамтамасыз ету.

4) Қол жеткізуді басқару: Университеттің аппараттық, бағдарламалық, ақпараттық жүйелері мен ақпараттық ресурстарына қызметкерлердің рөлдері мен өкілеттіктеріне байланысты қол жеткізуді шектеу.

5) Деректердің резервтік көшірмесін жасау және қалпына келтіру жүйесін жақсарту: Критикалық маңызды ақпараттық ресурстар мен деректер базаларын сенімді қорғау және тез қалпына келтіру үшін резервтік көшірме жасау және қалпына келтіру жүйесін жаңарту.

6) Зиянды бағдарламалар мен қауіптерден қорғау: DDoS-шабуылдар, вирустар, зиянды бағдарламалар және ақпараттық қауіпсіздіктің басқа да қауіптері сияқты кибершабуылдардың зардаптарын болдырмау және азайту. Ақпараттық қауіпсіздікті басқару жүйесінің (АҚБЖ) инфрақұрылымын дамыту,

оның ішінде қазіргі заманғы қорғау құралдарын (фаерволдар, басқару жүйелері, антивирустық шешімдер және т.б.) орнату және баптау.

7) Аппараттық құралдарды жаңарту: Ескірген жабдықтарды (серверлер, желілік құрылғылар, деректер сақтау құрылғылары) қауіпсіздік сипаттамалары жақсартылған қазіргі заманғы модельдерге ауыстыру.

8) Бағдарламалық қамтамасыз етуді жақсарту: Операциялық жүйелерді, деректер базаларын, антивирустық бағдарламаларды және басқа да бағдарламалық қамтамасыз етуді қауіпсіздікке арналған соңғы жаңартулары бар өзекті нұсқаларға жаңарту.

9) Оқиғаларды басқару жүйесін жақсарту: Ақпараттық қауіпсіздік оқиғаларын нақты уақытта жинауға, талдауға және оларға жауап беруге мүмкіндік беретін оқиғаларды басқару жүйесін (SIEM) дамыту.

10) Заңнамаға және реттеулерге сәйкестік: Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамалық талаптары мен нормативтік-құқықтық актілерін орындау, ақпараттық қауіпсіздікті қамтамасыз ету және жеке деректерді қорғау бойынша нормативтік-құқықтық базаны әзірлеу және жетілдіру.

11) Оқыту және хабардар ету: Университет қызметкерлері арасында ақпаратты қорғау әдістері мен желідегі қауіпсіз мінез-құлық ережелері туралы хабардарлық деңгейін көтеру. Ақпараттық қауіпсіздік бойынша IT-мамандары мен әкімшілер үшін оқыту сертификаттау курстарын өткізу.

12) Оқиғаларға жауап беру: Ақпараттық қауіпсіздік оқиғаларына жауап беру бойынша нұсқауларды әзірлеу және іске асыру. Дағдарыстық (төтенше) жағдайлар салдарынан бағдарламалық және техникалық құралдардың, сондай-ақ ақпараттың жоғалуын азайту және қалпына келтіру. Мұндай жағдайлардың пайда болу себептерін тергеу және оларды болашақта болдырмау бойынша шаралар қабылдау.

13) Тәуекелдерді басқару: Ақпараттық қауіпсіздікке байланысты тәуекелдерді бағалау және басқару, өзгеріп отыратын қауіпті ортаны ескере отырып. Тәуекелдер деңгейін азайту және Университет қызметкерлерінің қателіктерінен, техникалық ақаулардан туындайтын ықтимал шығындарды азайту.

14) Қауіпсіздікті мониторингілеу: Ақпараттық қауіпсіздік оқиғаларын ерте анықтау және шабуылдарды болдырмау үшін қауіпсіздік оқиғаларын мониторингілеу. Ақпараттық қауіпсіздікті қамтамасыз ету үшін қолданылатын техникалық құралдар мен инфрақұрылымның қазіргі жағдайын бағалау. Ескірген немесе жеткіліксіз компоненттерді анықтау.

5 Тарау. АҚ принциптері

8. Университеттің ақпараттық қауіпсіздік принциптері ақпаратты әртүрлі қауіптерден қорғауды қамтамасыз ету үшін сақталуы тиіс негізгі принциптер мен тәсілдерді білдіреді:

1) Тұтастық: Бұл принцип ақпараттың дәлдігін, тұтастығын және толықтығын қамтамасыз етуді білдіреді. Ақпарат оның дұрыстығына немесе сенімділігіне әсер етуі мүмкін рұқсатсыз өзгертулерден немесе өзгертулерден қорғалуы тиіс.

2) Құпиялылық: Құпиялылық принципі құпия ақпаратқа тек өз жұмыс міндеттерін немесе тапсырмаларын орындау үшін қажетті рұқсат берілген пайдаланушыларға ғана қол жеткізуді талап етеді. Ақпаратқа рұқсатсыз қол жеткізуден қорғау құпиялылықты қамтамасыз етуде маңызды рөл атқарады.

3) Қолжетімділік: Қолжетімділік принципі ақпарат пен оған байланысты жүйелердің рұқсат берілген пайдаланушылар үшін қажетті уақытта және орында қолжетімді болуын қамтамасыз етеді.

4) Аутентификация: Аутентификация принципі ақпаратқа немесе ресурстарға қол жеткізуге әрекеттенетін пайдаланушылардың, құрылғылардың немесе жүйелердің шындығын тексеруді білдіреді. Бұл пайдаланушыларды анықтау үшін парольдерді, электрондық цифрлік қолтаңбаны және басқа әдістерді қолдануды қамтиды.

5) Авторизация: Авторизация принципі рұқсат берілген пайдаланушылардың белгілі бір ресурстар мен деректерге қол жеткізу құқықтары мен артықшылықтарын айқындайды.

6) Қызмет көрсетуден бас тарту мүмкін еместігі: Қызмет көрсетуден бас тарту мүмкін еместігі принципі жіберуші немесе алушының хабарламаны немесе деректерді жіберу немесе алу фактісін жоққа шығара алмайтындығын кепілдейді. Бұл аутентификация арқылы қамтамасыз етіледі.

7) Міндеттерді бөлу: Міндеттерді бөлу принципі жүйелік артықшылықтарды теріс пайдалану мүмкіндігін болдырмау үшін маңызды функцияларды әртүрлі қызметкерлер немесе топтар арасында бөлуге бағытталған.

8) Деректерді бөлу: Деректерді бөлу принципі сезімтал деректерді аз сезімтал немесе қоғамдық деректерден бөлу арқылы ақпараттың ағуының тәуекелдерін азайтуға көмектеседі.

9) Жеке жауапкершілік: Бұл принцип бойынша қызметкерлердің құқықтары мен міндеттерінің бөлінуі кез келген бұзушылық жағдайында кінәлілер шеңбері нақты белгілі немесе ең азға дейін азайтылған болуы тиіс.

10) Заңдылық: Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамалық талаптарын сақтау.

6 Тарау. АҚ тәжірибелік тәсілдері

9. Ақпараттық қауіпсіздіктің тәжірибелік тәсілдері ақпаратты, деректер базаларын және ақпараттық жүйелерді әртүрлі қауіптерден қорғауда маңызды рөл атқарады. Университетте қолданылатын негізгі тәжірибелік тәсілдер:

1) Пайдаланушыларды оқыту және хабардар ету: Пайдаланушыларды интернеттегі қауіпсіз мінез-құлықтың негіздері, фишингтік шабуылдардан, парольдерді қорғаудан және т.б. бойынша оқыту.

2) Қол жеткізуді басқару: Рұқсат берілген пайдаланушылардың Университеттің электрондық ақпараттық ресурстары мен ақпараттық жүйелеріне қол жеткізу құқықтарын анықтау және рөлдерді тағайындау.

3) Бағдарламалық қамтамасыз етуді жаңарту: Операциялық жүйелерді, қолданбалы бағдарламалық қамтамасыз етуді және антивирустық бағдарламаларды соңғы нұсқаларға дейін үнемі жаңарту. Белгілі осалдықтарды жабу үшін қауіпсіздік түзетулерін орнату.

4) Деректерді шифрлау: Деректерді сақтау және желі арқылы беру кезінде шифрлауды қолдану. Құпия деректерді қорғау үшін дисктер мен файлдарды шифрлауды іске асыру.

5) Деректердің резервтік көшірмесін жасау: Деректердің резервтік көшірмелерін үнемі жасау және оларды қорғалған орындарда сақтау.

6) Оқиғаларды мониторингілеу және тіркеу: Аномалиялар мен ықтимал қауіпсіздік оқиғаларын анықтау үшін қауіпсіздік мониторингі жүйесін қолдану. Оқиғаларды талдау және тіркеу арқылы қауіптерге оперативті жауап беру.

7) Физикалық қауіпсіздік: Сервер бөлмелерінің физикалық қауіпсіздігін қамтамасыз ету. Университетте қол жеткізуді бақылау және бейнебақылау жүйелерін қолдану.

8) Зиянды бағдарламалар мен кибершабуылдардан қорғау: Барлық компьютерлер мен серверлерде антивирустық бағдарламалар мен файерволдарды орнату.

9) Қауіпсіздікті мониторингілеу: Университеттің электрондық ақпараттық ресурстарын, ақпараттық жүйелерін және деректер базаларын қауіпсіз пайдалануды мониторингілеуге бағытталған ұйымдастырушылық және техникалық шаралар.

10) Нормативтік талаптарды сақтау: Қазақстан Республикасының заңнамасы және Университеттің ішкі құжаттары бойынша белгіленген деректерді қорғау талаптарын орындау.

7 Тарау. Жауапкершілік

10. Барлық қызметкерлер Университеттің ақпараттық ресурстарын білікті, тиімді пайдалануға және этика ережелеріне сәйкес әрекет етуге міндетті.

11. Университеттің басшылығы ақпараттық қауіпсіздік саясатын іске асыру үшін қажетті ресурстарды, оның ішінде оқытуды қаржыландыруды, қажетті технологиялар мен қорғау құралдарын енгізуді қамтамасыз етеді.

12. Құрылымдық бөлімшелердің басшылары қызметкерлерді ақпараттық қауіпсіздік саясатымен таныстыру үшін жеке жауапкершілік тартады және ақпараттық қауіпсіздік талаптарын бұзуға байланысты барлық оқиғалар мен күдікті жағдайлар туралы Университеттің ақпараттық қауіпсіздікке жауапты қызметкерге дереу хабарлауға міндетті.

13. Қауіпсіздік саясатын енгізу және қолдау Университеттің барлық қатысушыларының, басшылықтан бастап, ақпараттық жүйелердің

пайдаланушыларына дейінгі бірлескен күш-жігері болып табылады. Бұл деректердің сыртқа шығуы, қауіпсіздіктің бұзылуы сияқты тәуекелдерді азайтуға және университеттің құнды ақпаратын қорғауға көмектеседі.

14. Ақпараттық қауіпсіздік саласындағы жергілікті нормативтік актілердің талаптарын бұзу үшін жауапкершілік дәрежесі әрбір нақты жағдайда анықталады.

8 Тарау. Өзгертулер енгізу тәртібі

15. Осы Саясатқа өзгерістер енгізу бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімі бастығының, персоналды басқару бөлімі бастығының, жетекшілік ететін проректордың бастамасы бойынша жүзеге асырылады және ҚП 082-2022 Құжаттау процедурасы. Құжаттаманы басқару ережесіне сәйкес жасалады.

9 Тарау. Келісу, сақтау және тарату

16. Келісу, сақтау және тарату ҚП 082-2022 Құжаттау процедурасы. Құжаттаманы басқару құжатына сәйкес жасалады

17. Осы Саясат зерттеулер, инновациялар және цифрландыру жөніндегі проректормен, құқықтық қамтамасыз ету және мемлекеттік сатып алулар бөлімінің басшысымен, персоналды басқару бөлімінің басшысымен және құжаттаманы қамтамасыз ету бөлімінің басшысымен келісіледі.

18. Осы Саясаттың түпнұсқасы «Келісім парағымен» бірге қабылдау-тапсыру актісі бойынша ПББ-ға сақтауға беріледі.

19. Осы Саясаттың жұмыс данасы университеттің веб-сайтында ішкі корпоративтік желіден кіру мүмкіндігімен орналастырылады.