КГУ «Управление архитектуры, градостроительства и земельных отношений города Нур-Султан»

УТВЕРЖДЕНО

Директор ТОО «АстанаГорАрхитектура» города Нур-Султан

_____ Кенжебеков Н. К.

«__19__» _октября_ 20_20_ г.

М. П.

УТВЕРЖДЕНО

Руководитель Управления архитектуры, градостроительства и земельных отношений города Нур-Султан

_____ Уранхаев Н. Т.

«__19__» _октября_ 20_20_ г.

М. П.

Правила использования мобильных устройств и носителей информации Информационной системы «Геоинформационный портал города Нур-Султан» ГПГ.СМИБ.ПР.12.r02.20

г. Нур-Султан
2020 г.

1. Область применения

Целью настоящего документа является описание правил использования мобильных устройств и носителей информации, и определение порядка действий ответственных сотрудников Организации, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта ИС.

2. Нормативные ссылки

Настоящий документ содержит указания к практическому исполнению требований, изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

3. Термины, определения и сокращения

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

4. Общие положения

Настоящий документ определяет правила и порядок обращения с носителями информации, а также порядок проверки и защиту документов, компьютерных носителей информации (лент, дисков), данных ввода/вывода и системной документации от повреждения, воровства и неправомочного доступа, является Правила использования мобильных устройств и носителей информации.

Под использованием мобильных устройств и носителей информации в информационных ресурсах Организации понимается их подключение к инфраструктуре информационных ресурсов с целью обработки, приема/передачи информации между информационными ресурсами и мобильными устройствами, а также носителями информации.

В виду того, что носители информации могут хранить конфиденциальную информацию и персональные данные сотрудников проекта и пользователей ИС, настоящий документ описывает адекватные меры учета, хранения и обращения со съемными носителями, а так же их безопасную утилизацию.

Обязанности по контролю исполнения требований ИБ настоящего раздела возлагаются на ответственного за обеспечение ИБ.

При использовании переносных устройств, например ноутбуков, карманных компьютеров, переносных компьютеров и мобильных телефонов, необходимо принимать специальные меры противодействия компрометации служебной информации. Настоящий документ формализует политику, учитывающую риски, связанные с работой с переносными устройствами, в особенности в незащищенной среде.

Настоящий документ включать в себя требования по физической защите, контролю доступа, использованию средств и методов

криптографии, резервированию и защите от вирусов. Настоящий документ также содержит правила и рекомендации по подсоединению мобильных средств к сетям, а также инструкции по использованию этих средств в общедоступных местах.

СОИБ несет ответственность за информирование сотрудников, использующих переносные устройства, о дополнительных рисках и необходимых мероприятиях обеспечения информационной безопасности, связанных с этим способом работы.

5. Использование мобильных устройств и носителей информации

Требования к сотрудникам при использовании съемных носителей

Сотрудникам проекта разрешается использовать только служебные мобильные устройства, и только служебные носители информации. Использование персональных мобильных устройств и носителей информации для подключения к сети проекта или обработки, хранения и передачи служебной информации строго запрещено.

Сотрудники проекта должны проявлять осторожность при использовании мобильных средств вычислительной техники и других сервисных средств в общедоступных местах, переговорных комнатах и незащищенных помещениях вне защищенных помещениях проекта. Чтобы исключить неавторизованный доступ или раскрытие информации, хранимой и обрабатываемой этими средствами, необходимо (в тех случаях если это целесообразно) использование средства и методы защиты информации.

При использовании мобильных средств в общедоступных местах важно проявлять осторожность, чтобы уменьшить риск «подсмотра» паролей доступа неавторизованными лицами. Необходимо использовать и поддерживать в актуализированном состоянии средства и способы защиты от вредоносного программного обеспечения.

Соответствующую защиту необходимо обеспечивать мобильным средствам, подсоединенным к общедоступным сетям. Удаленный доступ к служебной информации через общедоступную сеть с использованием мобильных средств вычислительной техники следует осуществлять только после успешной идентификации и аутентификации, а также при наличии соответствующих механизмов управления доступом.

При использовании сотрудниками служебных носителей информации необходимо:

- соблюдать требования настоящего документа;
- использовать служебные носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность ответственного за обеспечение ИБ о любых фактах нарушения требований настоящего документа;

– бережно относится к служебным носителям информации;

– обеспечивать физическую безопасность носителей информации всеми разумными способами;

– в случае утраты или выходе из строя служебных носителей информации или при подозрении о компрометации хранимой информации на служебном носителе извещать ответственного за обеспечение ИБ.

Сотрудникам запрещается

– использовать носители конфиденциальной информации в личных целях;

– передавать носители конфиденциальной информации другим лицам;

– хранить съемные служебные носители информации в незащищенном, оставлять на рабочих столах, оставлять их без присмотра или передавать на хранение другим лицам

– выполнять антивирусную проверку съемных носителей при каждом подключении к служебной рабочей станции.

Переносные устройства необходимо также физически защищать от краж, особенно когда их оставляют без присмотра, забывают в автомобилях или других видах транспорта, гостиничных номерах, конференц-залах и других местах встреч. В случай кражи или потери переносных устройств ответственный за них сотрудник должен уведомить СОИБ и руководство Организации. Оборудование, на котором хранится важная и/или критическая коммерческая информация, нельзя оставлять без присмотра и по возможности необходимо физически изолировать его в надежное место или использовать специальные защитные устройства на самом оборудовании, чтобы исключить его неавторизованное использование

Служебные носители информации, пришедшие в негодность, или отслужившие установленный производителем срок, подлежат утилизации в порядке, установленном настоящим документом и Правилами инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения.

Управление съемными носителями информации

К съемным носителям относятся магнитные ленты, диски, флэш-диски, съемные жесткие диски, компакт-диски, DVD-диски и печатные носители.

Для управления съемными носителями информации применяются следующие мероприятия по управлению информационной безопасностью:

а) если носители информации многократного использования больше не требуются и передаются за пределы организации, то их содержимое должно быть уничтожено, с использованием методов

безвозвратного уничтожения информации применимого к этому типу носителя;

b) вынос носителей информации за пределы организации должен быть документирован, и разрешен ответственным за обеспечение ИБ (см. раздел 9 Правил идентификации, классификации и маркировки активов, связанных со средствами обработки информации);

c) все носители информации следует хранить в надежном, безопасном месте в соответствии с требованиями изготовителей;

d) информация, хранимая на носителях и требующая хранения после истечения срока годности (в соответствии с техническими характеристиками), должна храниться в надежном месте во избежание потери информации вследствие износа носителя;

e) при использовании носителей следует учитывать срок эксплуатации, указанный производителем;

f) доступ к устройствам чтения носителей информации должен быть подотчетным, документируемым и авторизованным;

g) процессы хранения и обращения со съемными носителями должны учитывать требования производителей к среде функционирования и хранения носителей информации;

h) выдача и возврат цифровых носителей информации должны фиксироваться в журнале выдачи носителей информации и мобильных устройств (по форме Приложения 2).

i) При использовании мобильных устройств и носителей за пределами организации имеется риск распространения служебной информации работниками.

j) Защита мобильного оборудования, находящегося за пределами рабочего места осуществляется аналогично стационарным ПК в соответствии с Едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

Следующие требования необходимо исполнять для защиты удаленного оборудования:

a) оборудование и данные, которые получены вне территории организации, не должны быть оставлены без присмотра в общественных местах;

b) инструкции изготовителей для защиты оборудования должны проверяться в любом случае, например, защита от воздействия сильных электромагнитных полей;

c) средства управления для рабочих мест вне организации, таких как надомная работа, удаленные и временные места должны быть определены оценкой степени риска и подходящими средствами управления. Например, запирающиеся шкафы для хранения документов, ясная политика стола, средства управления доступом для компьютеров и безопасная связь с офисом;

d) когда оборудование вне помещения распространено среди различных людей или третьих сторон, регистрация должна сохраняться, которая позволит определить имена и организации тех, кто ответственен за оборудование. Риски, например, повреждения, воровство или подслушивания, могут измениться значительно между местоположениями и должны быть приняты во внимание в определении самых соответствующих средств управления.

Порядок учета, хранения и обращения со съемными носителями информации и мобильными устройствами

Все служебные носители информации и служебные мобильные устройства должны быть промаркированы, и закреплены за ответственным сотрудником и учтены в Журнале учета съемных носителей информации и мобильных устройств (по форме Приложения 1).

Учет и выдачу служебных носителей информации и служебных мобильных устройств осуществляет ответственный за обеспечение ИБ. Факт выдачи съемного носителя фиксируется в журнале выдачи носителей информации и мобильных устройств (по форме Приложения 2).

Съемные носители информации и мобильные устройства должны храниться в защищенном месте, доступ к которому может иметь только авторизованный персонал. Съемные носители информации и мобильные устройства должны очищаться от хранимой информации (сбрасываться до заводских настроек) перед и после передачи в пользование сотруднику проекта ИС или при смене пользователя.

Хранение и обращение со съемными носителями информации и мобильными устройствами должны соответствовать требованиям документов ИБ проекта ИС и требованиям производителей оборудования.

При хранении и обращении со съемными носителями информации и мобильными устройствами сотрудники проекта ИС должны соблюдать требования настоящего документа.

Утилизация носителей информации

Носители информации по окончании использования следует надежно и безопасно утилизировать. Важная информация может попасть в руки посторонних лиц из-за небрежной утилизации носителей данных.

При утилизации или смены места использования носителей информации необходимо учитывать следующее:

a) носители, содержащие важную информацию, следует хранить и утилизировать надежно и безопасно (например, посредством сжигания/измельчения). Если носители информации планируется использовать в пределах организации для других задач, то информация на них должна быть уничтожена;

b) при смене места использования носителя информации, должна быть произведена смена маркировки носителя;

c) при смене места использования носителя информации должен быть указан ответственный сотрудник;

d) в случае необходимости следует прибегнуть к сторонним поставщикам услуг уничтожения носителей информации, однако процесс уничтожения должен контролироваться ответственным за обеспечение ИБ;

e) необходимо регистрировать утилизацию важных объектов с целью последующего аудита.

При накоплении носителей информации, подлежащих утилизации, следует применять соответствующие меры по их защите.

Ответственный за обеспечение ИБ не должен допускать компрометации информации в результате небрежной утилизации носителей информации (см. пп. 9.2.6, информация об утилизации использованного оборудования Политики ИБ).

Подготовки к повторному использованию носителей информации и мобильных устройств

Все оборудование, содержащее носители данных, должно быть проверено, чтобы гарантировать, что любые уязвимые данные и лицензированное программное обеспечение было удалены или надежно переписано до распоряжения или повторного использования.

Носители данных, содержащие конфиденциальную или защищенную авторским правом информацию, должны быть физически разрушены, или информация должна быть разрушена, удалена, или переписана с помощью техник, которые делают оригинальную информацию невосстановимой.

Носители информации и мобильные устройства перед повторным использованием следует надежно и безопасно отчистить от имеющейся информации. Важная информация может попасть в руки посторонних лиц из-за небрежного отношения к подготовке к повторному использованию.

Назначенный ответственный сотрудник за носитель информации или мобильное устройство должен использовать специальные программные средства безвозвратного удаления информации и/или штатные средства мобильного устройства для сброса до заводских настроек и отчистки встроенной памяти.

По окончании процедуры ответственный сотрудник должен сделать соответствующую запись в Журнал выдачи/возврата/утилизации и подготовки к повторному использованию носителей информации, мобильных устройств, серверного и телекоммуникационного оборудования, систем хранения данных и рабочих станций.

Сотрудник, принимающий в пользование носитель информации или мобильное устройство, должен убедиться в том, что в Журнале выдачи/возврата и подготовки к повторному использованию носителей информации и мобильных устройств имеется запись о его безопасной отчистке. Если такой записи нет, он не должен принимать устройство пока оно не будет подготовленно должным образом.

На СОИБ возлагается ответственность за контроль процедуры подготовки к повторному использованию носителей информации и мобильных устройств.

6. Процедура утилизации и/или подготовки к повторному использованию серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций

Утилизация серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций

При подготовке к утилизации серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций следует руководствоваться требованиями настоящего документа к процедуре утилизации носителей информации.

Ответственный за обеспечение ИБ не должен допускать компрометации информации в результате небрежной утилизации носителей информации (см. пп. 9.2.6, информация об утилизации использованного оборудования Политики ИБ).

Подготовки к повторному использованию серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций

Все оборудование, содержащее носители данных, должно быть проверено, чтобы гарантировать, что любые уязвимые данные и лицензированное программное обеспечение было удалены или надежно переписано до распоряжения или повторного использования.

Носители данных, содержащие конфиденциальную или защищенную авторским правом информацию, должны быть физически разрушены, или информация должна быть разрушена, удалена, или переписана с помощью техник, которые делают оригинальную информацию невосстановимой.

Серверное и телекоммуникационное оборудование, системы хранения данных, рабочие станций перед повторным использованием следует надежно и безопасно отчистить от имеющейся информации. Важная информация может попасть в руки посторонних лиц из-за небрежного отношения к подготовке к повторному использованию.

Назначенный ответственный сотрудник за устройство должен использовать специальные программные средства безвозвратного удаления информации со все носителей информации устройства и/или штатные средства устройства для сброса до заводских настроек и отчистки всех носителей информации устройства.

По окончании процедуры ответственный сотрудник должен сделать соответствующую запись в Журнал выдачи/возврата/утилизации и подготовки к повторному использованию носителей информации, мобильных устройств, серверного и телекоммуникационного оборудования, систем хранения данных и рабочих станций.

Сотрудник, принимающий в пользование устройство, должен убедиться в том, что в Журнал выдачи/возврата/утилизации и подготовки к повторному использованию носителей информации, мобильных устройств, серверного и телекоммуникационного оборудования, систем хранения данных и рабочих станций имеется запись о его безопасной отчистке. Если такой записи нет, он не должен принимать устройство пока оно не будет подготовленно должным образом.

На СОИБ возлагается ответственность за контроль процедуры подготовки к повторному использованию серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций.

7. Порядок действий при выявлении фактов несанкционированных действий сотрудников при использовании, а также при утрате и уничтожении съемных носителей

Действия при утрате.

В случае утраты съемного носителя сотрудник ответственный за носитель информации обязан незамедлительно обратиться к ответственному за обеспечение ИБ. СОИБ вместе с сотрудником ответственным за носитель информации должны предпринять меры по поиску утраченного носителя, если это возможно.

Если носитель не был найден, ответственный за носитель информации обязан написать объяснительную записку на имя руководителя Организации.

Объяснительная записка должна содержать:

a) изложение событий приведших к инциденту ИБ;
b) ориентировочные место и время утраты;
c) присутствующие лица (по возможности их контакты);
d) опись хранимой информации.

Ответственный за обеспечение ИБ проводит анализ рисков утерянной информации и представляет отчет руководству Организации.

На основе отчета о рисках, руководство Организации принимает решении о целесообразности обращения в правоохранительные органы для дальнейших поисков.

Действия при уничтожении.

В случае уничтожения, повреждения, выхода из строя съемного носителя сотрудник ответственный за носитель информации обязан незамедлительно обратиться к ответственному за обеспечение ИБ.

Сотрудник ответственный за носитель информации обязан предоставить ответственному за обеспечение ИБ остатки носителя информации.

СОИБ должен произвести сверку полученных остатков носителя информации с записями журнал выдачи носителей информации и

мобильных устройств и выполнить процедуру утилизации или передать на ремонт в соответствии с требованиями и в порядке установленном настоящим документом и Правилами инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения..

Действия при выявлении фактов несанкционированных действий со съемными носителями.

В случае если сотрудник Проекта ИС стал свидетелем несанкционированных действий со съемными носителями информации он обязан незамедлительно обратиться к ответственному за обеспечение ИБ и написать объяснительную записку на имя руководителя Организации.

Объяснительная записка должна содержать:

a) изложение событий приведших к инциденту ИБ;
b) место и время инцидента;
c) присутствующие лица (по возможности их контакты);
d) указание лица, совершившего несанкционированные действия.

Ответственный за обеспечение ИБ обязан изъять из использования служебный носитель информации. Произвести сверку полученного носителя информации с записями журнал выдачи носителей информации и определить сотрудника ответственного за носитель информации. Провести анализ рисков скомпрометированной информации и представить отчет руководству Организации.

На основе отчета о рисках, руководство Организации принимает решении о целесообразности обращения в правоохранительные органы, применения административных или дисциплинарных мер в соответствии с законодательством РК.

Процедуры обработки информации

Для обеспечения безопасности информации в процессе обработки, с соблюдением установленных категорий (пп. 7.2 Политики), применяются следующие меры:

a) обработка и маркирование всех носителей информации;
b) ограничения доступа с целью идентификации неавторизованного персонала;
c) ограничение по времени процедуры авторизации пользователей;
d) обеспечение уверенности в том, что данные ввода являются полными, процесс обработки завершается должным образом и имеется подтверждение вывода данных;
e) обеспечение защиты информации в процессе ввода, передачи, хранения и вывода;
f) хранение носителей информации в соответствии с требованиями изготовителей;
g) выполнение регулярного пересмотра прав доступа и списка допущенных к информации лиц;

h) четкую маркировку всех копий данных, предлагаемых вниманию авторизованного получателя;

i) регулярный пересмотр списков рассылки и списков авторизованных получателей.

Доступ к любой информации предоставляется только с письменного запроса и письменного разрешения руководства Организации или уполномоченного им лица.

Привилегии доступа учитывают категорирования информации, а также в отношении документов, вычислительных систем, сетей, переносных компьютеров, мобильных средств связи, почты, речевой почты, речевой связи вообще, мультимедийных устройств, использования факсов и любых других важных объектов, например, бланков, чеков и счетов, и любых других носителей информации и видов ее представлении

Безопасность системной документации

Документация, утверждённая в Организации, должна хранится в защищенном месте, предоставляться авторизованным сотрудникам согласно их функциональным обязанностям под роспись, выдача документации должна фиксироваться в журнале ознакомления с документами (по форме Приложения 2 Политики).

Оригиналы документов должны храниться в защищенном месте, для ознакомления и работы должны выдаваться рабочие экземпляры (копии документов). Все рабочие экземпляры должны быть пронумерованы, прошнурованы и подотчетны.

С целью защиты документации от несанкционированного доступа необходимо применять следующие мероприятия:

a) документацию следует хранить безопасным образом;

b) список лиц, имеющих доступ к документации, следует сводить к минимуму; доступ должен быть авторизован ответственным за обеспечение ИБ;

c) документация, передаваемая через общедоступную сеть, должна шифроваться.

8. Ответственность

СОИБ несет ответственность за:

a) контроль исполнения требований настоящего документа,

b) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

a) исполнение настоящей Инструкции.

Пользователи ИС:

a) исполнение настоящей Инструкции.

Приложение 1

Журнал учета съемных носителей информации и мобильных устройств Информационной системы «Геоинформационный портал города Нур-Султан» ГПГ.СМИБ.ПР.12-01.r02.20

№ п/п	Дата постановки на учет/ уничтожения	Вид, модель носителя	Серийный/ инвентарный номер/ уникальный идентификатор	Разрешенная к хранению категория информации	Место хранения	Отметка об уничтожении носителя	Должность/ФИО/подпись ответственного за носитель/устройство
1	2	3	4	5	6	7	8

Приложение 2

Журнал выдачи/возврата/утилизации и подготовки к повторному использованию носителей информации, мобильных устройств, серверного и телекоммуникационного оборудования, систем хранения данных и рабочих станций
Информационной системы «Геоинформационный портал города Нур-Султан»
ГПГ.СМИБ.ПР.12-02.r02.20

№ п/п	Серийный/ инвентарный номер/ уникальный идентификатор	Ф. И. О	Должность	Принял/ вернул/утилизировал/ подготовил к повторному использованию	Роспись
1	2	3	4	5	6