Политика
информационной безопасности АО «Jusan Mobile»

Информация является активом, который, подобно другим важным деловым активам, имеет большое значение для бизнеса организации и, следовательно, должен быть адекватно защищен.

Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость.

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности.

Раздел 1. ОБЩАЯ ПОЛИТИКА

1. Политика разработана с целью определения основных принципов и направлений в области информационной безопасности и охватывает все бизнес-процессы, информационные системы и документы, владельцем и пользователем которых является Общество.

2. Целью деятельности по управлению информационной безопасностью в Обществе является обеспечение конфиденциальности, целостности, доступности и защиты информационных активов Общества и минимизация ущерба от событий, таящих угрозу безопасности информации.

3. Политика разработана в соответствии с требованиями пунктов 31 и 33 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 и стандарта ISO/IEC 27001

4. Основными задачами деятельности по управлению информационной безопасностью в Обществе являются:

- категорирование информационных активов путем разделения их на критичные и некритичные на основании уровня критичности, хранимой и обрабатываемой в них информации;
- своевременное выявление потенциальных угроз информационной безопасности и уязвимостей в информационных активах Общества;
- исключение либо минимизация выявленных угроз;

- предотвращение инцидентов информационной безопасности или минимизация их последствий.

5. Основными мерами защиты конфиденциальности, целостности и доступности информационных активов Общества являются:

– управление сетевой безопасностью;
– управление уязвимостями и политиками безопасности;
– управление безопасностью конечных устройств;
– управление идентификацией и доступом;
– управление инцидентами информационной безопасности;
– управление криптографическими средствами защиты;
– управление антивирусными средствами защиты;
– обеспечение физической безопасности информационных активов;
– обеспечение безопасности при взаимодействии с контрагентами;
– обучение и повышение осведомленности персонала в вопросах ИБ;
– обеспечение безопасности интернет-ресурсов;
– обеспечение безопасности персональных данных.

Раздел 2. ОСОБЕННЫЕ ПОЛОЖЕНИЯ

1. Общество обеспечивает создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления Общества, предназначенной для управления процессом обеспечения информационной безопасности.

2. Построение системы управления информационной безопасности в Обществе и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства РК и собственных требований Общества, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Общества;

- ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки бизнес-процессов в Обществе. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности Общества;

- непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Общества должны осуществляться без прерывания или остановки текущих бизнес-процессов Общества;

- комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

- обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам;

- приоритетность – категорирование (ранжирование) всех информационных ресурсов Общества по степени критичности на основании уровня критичности хранимой и обрабатываемой в них информации, а также потенциальных угроз информационной безопасности;

- необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им функциональных обязанностей в рамках своих полномочий;

- специализация – эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными работниками Общества;

- информированность и персональная ответственность – руководители всех уровней и работники Общества должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;

- взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений Общества, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

- подтверждаемость – критичная документация и все записи – документы, подтверждающие исполнение требований по информационной безопасности и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

3. Основными задачами по обеспечению информационной безопасности и сохранности конфиденциальной информации являются:

- обеспечение необходимой доступности информационных ресурсов АО «Jusan Mobile» в целях обеспечения непрерывности бизнеса;
- обеспечение целостности информационных ресурсов АО «Jusan Mobile» в целях обеспечения требуемой поддержки деятельности АО «Jusan Mobile» в информационной сфере, включая задачи принятия решений;
- обеспечение конфиденциальности информации, отнесенной к закрытым сведениям АО «Jusan Mobile»;
- обеспечение достоверности и актуальности обрабатываемой информации;
- установление ответственности за использование информационных активов АО «Jusan Mobile» и управления ими;
- применение обоснованных, экономически выгодных и совместимых организационных и технических мер ИБ, как для информационных технологий, так и для АО «Jusan Mobile» в целом;
- применение обоснованных, организационных мер в вопросах информационной безопасности, поддерживающей осведомленность работников;
- защиту законных прав АО «Jusan Mobile» и работников, в случаях неправомерного использования или злоупотребления информационными активами;
- защиту от несанкционированных действий в процессах функционирования информационных систем;
- разграничение прав доступа к информации, серверам и рабочим станциям, средствам защиты.
- защита персональных данных в АО «Jusan Mobile» осуществляется в соответствии с законом «О персональных данных и их защите» и нормативными правовыми актами Республики Казахстан, принятыми в реализацию закона.

4. Общество разрабатывает внутренние процедуры по созданию, сбору, хранению и обработке информации в информационных системах Общества. Общества осуществляет мониторинг за процессами создания, хранения и обработки информации и доступа к ней с помощью механизмов информационных систем и технических средств обеспечения безопасности. Доступ к создаваемой, хранимой и обрабатываемой информации в информационных системах Общества предоставляется работникам в соответствии с их функциональными обязанностями в соответствии с принципом наименьшего уровня привилегий.

5. Участниками системы управления информационной безопасностью Общества являются все структурные подразделения.

При работе с поставщиками доступ к информации для поставщиков предоставляется в объеме, необходимом и достаточном для исполнения их задач согласно соответствующему договору после подписания соглашения о неразглашении конфиденциальной информации.

Работники Компании ознакамливаются с требованиями правил АО «Jusan Mobile» и принятых процедурах, включая требования к информационной безопасности и другим средствам контроля, а также обучены правильно использовать информационные ресурсы и сервисы информационных систем.

Работник обязан хранить в тайне ставшие ему известными по работе конфиденциальные сведения, а также пресекать действия других лиц, которые могут привести к разглашению таких сведений.

Работник Компании со дня приема на работу подписывает документ о неразглашении сведений, составляющих конфиденциальную информацию, а также проходит инструктаж по вопросам информационной безопасности.

Руководство Общество принимает непосредственное участие в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами.

Руководство Общество на постоянной основе осуществляет поддержку заданного уровня информационной безопасности путем внедрения системы менеджмента в полном соответствии стандарту ISO/IEC 27001, а также обязуется постоянно улучшать систему информационной безопасности.

Раздел 3. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

1. Ответственность за неисполнение/ненадлежащее исполнение требований Политики, а также за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей несут все работники Общества.
2. Контроль за исполнением требований, устанавливаемых Политикой, возлагается на подразделение информационной безопасности.

Отправлен автором
17.12.2025 16:27 Тукеев Жулдыз Жанатович
Действителен Уникальное имя владельца: ТУКЕЕВ ЖУЛДЫЗ Дата начала: 2025-01-21 11:34:42 (+05) Дата окончания: 2026-01-21 11:34:42 (+05) Серийный номер: 489682006198018122934505651674379442514593550732 Субъект: GIVENNAME=ЖАНАТОВИЧ, C=KZ, SERIALNUMBER=IIN870717302575, SURNAME=ТУКЕЕВ, CN=ТУКЕЕВ ЖУЛДЫЗ Издатель: C=KZ, CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022
Согласовано
17.12.2025 16:51 Шишова Алия Косеновна
Действителен Уникальное имя владельца: ШИШОВА АЛИЯ Дата начала: 2025-05-27 17:12:07 (+05) Дата окончания: 2026-05-27 17:12:07 (+05) Серийный номер: 12958093288725829861430629710639244526381351071З Субъект: GIVENNAME=КОСЕНОВНА, OU=BIN960340000405, O="Акционерное общество \"Jusan Mobile\"", C=KZ, SERIALNUMBER=IIN770314401813, SURNAME=ШИШОВА, CN=ШИШОВА АЛИЯ Издатель: C=KZ, CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022
18.12.2025 10:57 Жакутов Эрик Ануарович
Действителен Уникальное имя владельца: ЖАКУТОВ ЭРИК Дата начала: 2025-07-02 15:12:28 (+05) Дата окончания: 2026-07-02 15:12:28 (+05) Серийный номер: 13050549981888385534786153399439863295202903222б Субъект: GIVENNAME=АНУАРОВИЧ, OU=BIN960340000405, O="Акционерное общество \"Jusan Mobile\"", C=KZ, SERIALNUMBER=IIN730502301801, SURNAME=ЖАКУТОВ, CN=ЖАКУТОВ ЭРИК Издатель: C=KZ, CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022
18.12.2025 12:16 Бакырбаева Алия Нурбулатовна
Действителен Уникальное имя владельца: БАКЫРБАЕВА АЛИЯ Дата начала: 2025-06-03 11:18:15 (+05) Дата окончания: 2026-06-03 11:18:15 (+05) Серийный номер: 614547819977867426568925819185030507126569370050 Субъект: GIVENNAME=НУРБУЛАТОВНА, C=KZ, SERIALNUMBER=IIN780421400511, SURNAME=БАКЫРБАЕВА, CN=БАКЫРБАЕВА АЛИЯ Издатель: C=KZ, CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022
Утверждено
29.12.2025 15:38 Джексенов Ринат Александрович
Действителен Уникальное имя владельца: ДЖЕКСЕНОВ РИНАТ Дата начала: 2025-11-11 13:40:27 (+05) Дата окончания: 2026-11-11 13:40:27 (+05) Серийный номер: 14952524149959668731832959669359233315511217986б Субъект: GIVENNAME=АЛЕКСАНДРОВИЧ, OU=BIN960340000405, O="Акционерное общество \"Jusan Mobile\"", C=KZ, SERIALNUMBER=IIN850218351125, SURNAME=ДЖЕКСЕНОВ, CN=ДЖЕКСЕНОВ РИНАТ Издатель: C=KZ, CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022

Тип документа	ВНД
Номер и дата документа	№ ПР-37608 от 17.12.2025 г.
Организация/ отправитель	ГРУППА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Получатель (-и)	ЕЛШИЕВА Б.К.
Электронные цифровые подписи документа	Физическое лицо Отправлен автором: ТУКЕЕВ ЖУЛДЫЗ MIIPCwYJ...BHb5NHWoG Тип: НУЦ Время подписи: 17.12.2025 16:27
	Акционерное общество "Jusan Mobile" Согласовано: ШИШОВА АЛИЯ MIIPdwYJ...bid2Z/7h7 Тип: НУЦ Время подписи: 17.12.2025 16:51
	Акционерное общество "Jusan Mobile" Согласовано: ЖАКУТОВ ЭРИК MIIPewYJ...4FhSiGA== Тип: НУЦ Время подписи: 18.12.2025 10:57
	Физическое лицо Согласовано: БАКЫРБАЕВА АЛИЯ MIIPHQYJ...dRvGU9jiw Тип: НУЦ Время подписи: 18.12.2025 12:16
	Акционерное общество "Jusan Mobile" Утверждено: ДЖЕКСЕНОВ РИНАТ MIIPhgYJ...gSTNYy3Ib Тип: НУЦ Время подписи: 29.12.2025 15:38

Данный документ согласно пункту 1 статьи 7 ЗРК от 7 января 2003 года N370-II «Об электронном документе и электронной цифровой подписи», удостоверенный посредством электронной цифровой подписи лица, имеющего полномочия на его подписание, равнозначен подписанному документу на бумажном носителе.