КЕНЖЕҒАЛИ САҒАДИЕВ
АТЫНДАҒЫ
ХАЛЫҚАРАЛЫҚ БИЗНЕС
УНИВЕРСИТЕТІ

УНИВЕРСИТЕТ
МЕЖДУНАРОДНОГО БИЗНЕСА
ИМЕНИ КЕНЖЕГАЛИ
САГАДИЕВА

УТВЕРЖДЕНО
Ученым Советом УМБ
имени Кенжегали Сагадиева
Протокол № *7* от *20.01.2023*
Председатель Махметова А.М.

ПРАВИЛА

РЕГИСТРАЦИИ И ОТВЕТСТВЕННОСТИ ПОЛЬЗОВАТЕЛЯ В КОРПОРАТИВНОЙ СЕТИ

ТОО «УНИВЕРСИТЕТ МЕЖДУНАРОДНОГО БИЗНЕСА ИМЕНИ КЕНЖЕГАЛИ САГАДИЕВА»

ИЗДАНИЕ 1

Введено в действие с даты утверждения

Алматы, 2023

Оглавление

Паспорт документа

Тип документа	Организационная документация
Наименование документа	Правила регистрации и ответственности пользователя в корпоративной сети УМБ им. Кенжегали Сагадиева
Цель документа	Правила регулируют вопросы по поддержанию необходимого уровня безопасности защиты информации, ее сохранности, и соблюдения прав доступа к информационным ресурсам в корпоративной сети Университета им. Кенжегали Сагадиева
Разработка	Директором ДИТ
Согласование	Проректора по направлениям Директор ДАВ Декан факультета базового высшего образования Директор Graduate School of Business Директор Департамента человеческим по ресурсам и документации Руководитель Центра Обеспечения Качества Юрисконсульт
Утверждение	Председателем УС
Исполнители документа	Работники ДИТ/ДЦТ, структурные подразделения УМБ, Преподаватели и студенты УМБ
Контроль за исполнением	Первый руководитель УМБ
Приложения к документу	Нет
Нормативные ссылки	Политика разработан в соответствии с требованиями законодательства Республики Казахстан, Устава, а также внутренних нормативных и распорядительных документов ТОО «Университета международного бизнеса имени Кенжегали Сагадиева» 1. Закон Республики Казахстан «Об Образовании» *(с изменениями и дополнениями).* 2. Правила организации учебного процесса по кредитной технологии обучения, утвержденных приказом Министра образования и науки РК от 20.04.2011 № 152 *(с изменениями и дополнениями).*
Владелец оригинала	ДИТ

Лист согласования

Положение согласовано:

Проректор по науке
Нургалиева К. О. _____
«13» 01 2023 г.

Проректор по цифровизации
Мусабаев Н.Б. _____
«19» 01 2023 г.

Проректор по стратегии и социальному развитию:
Сабденалиев Б.А. _____
«19» 01 2023 г.

Директор ДАВ
Токина А.А. _____
«19» 01 2023 г.

Декан Факультета Базового Высшего Образования
Садыров Г.А. _____
«19» 01 2023 г.

Директор Graduate School of Business
Каликов М.А. _____
«19» 01 2023г.

Ио Директора Департамента человеческим по ресурсам и документации
Сихимбаева Г.М. _____
«19» 01 2023 г.

Руководитель Центра Обеспечения Качества
Кабдесов К.Т. _____
«19» 01 2023 г.

Юрисконсульт
Алибекова А.К. _____
«19» 01 2023 г.

Разработано:

Директор ДИТ
Фомичев С.В. _____
«19» 01 2023 г.

Редакция и оформление:

Project менеджер ЦОК
Дузбаева Р.М. _____
«19» 01 2023 г.

1. Общие положения

1.1 Настоящие Правила регистрации и ответственности пользователя в корпоративной сети ТОО «Университета международного бизнеса имени Кенжегали Сагадиева» (далее – Правила) разработаны в соответствии с требованиями законодательства Республики Казахстан, Устава, а также внутренних нормативных и распорядительных документов ТОО «Университета международного бизнеса имени Кенжегали Сагадиева» (далее – Университет).

1.2 Настоящие Правила регулируют вопросы по поддержанию необходимого уровня безопасности защиты информации, ее сохранности, и соблюдения прав доступа к информационным ресурсам в корпоративной сети Университета.

1.3 Настоящие Правила содержат необходимые требования по обеспечению:

1) регистрации пользователей в корпоративной сети Университета;

2) сохранности информации пользователей корпоративной сети;

3) соблюдение прав на распространение и защиту служебной и личной информации.

1.4 Системные администраторы сети и информационных систем Университета (далее по тексту - администраторы), при нарушении пользователем пункта 3.1 настоящих Правил имеют право останавливать процесс использования и передачи информации по сети для принятия мер по обеспечению безопасности сети. Процесс передачи информации может быть заблокирован на уровне учетной записи пользователя или на сетевом уровне (например - отключения рабочей станции (далее – РС) пользователя от корпоративной сети Университета).

1.5 Основные понятия, термины и сокращения, используемые в Правилах:

1) **ДИТ** – департамент информационных технологий;
2) **ДЧРиД** – департамент по человеческим ресурсам и документации;
3) **ДЦТ** – департамент цифровой трансформации;
4) **ККК** – квалификационная конкурсная комиссия;
5) **Лог-файлы сервера** — специальные файлы, в которых протоколируются определённые действия пользователя или программы на сервере;
6) **ИС** – информационные системы;
7) **ПО** – программное обеспечение;
8) **Пользователь** – любой сотрудник, преподаватель и студент Университета;
9) **РС** – рабочая станция, включая компьютер и монитор или моноблок;
10) **СП** – структурное подразделение (кафедра, деканат, ректорат)
11) **GLPI (Support.uib.kz)** – информационная система регистрации Заявок и Инцидентов.
12) **Фронт (Front.uib.kz) –** портал «электронный деканат» Университета.

2. Порядок регистрации, идентификации и авторизации пользователей

2.1 Работнику/преподавателю Университета при приеме на работу (после подписания Приказа о приеме на работу) предоставляется РС с установленным стандартным программным обеспечением, согласно нормативному документу Университета, регламентирующего предоставление доступов к ИС. Для предоставления доступов всем пользователям присваивается уникальный идентификатор (Логин) и Пароль, согласно требованиям Парольной политике Университета.

2.2 Для нового работника предоставление Логина и Пароля осуществляется вручную администраторам ДИТ. Для этого ответственный работник ДЧРиД оформляет

Заявку (форму прием на работу) в системе GLPI на предоставление доступов новому работнику. В заявке указываются необходимые данные согласно форме и вкладывается скан Приказа о приеме на работу. После этого администратор ДИТ заводит работника в систему Университета, предоставляет доступ к стандартным ИС и отсылает Логин и временный Пароль на личную почту нового работника. После этого заявка закрывается. Если работнику нужны дополнительные доступы в ИС Университета, то руководитель СП, в которое принимается новый работник, оформляет Заявку (форму предоставления доступов к ИС) в системе GLPI на предоставление доступов новому работнику. В заявке указывается подразделение, должность, Логин работника и указывается ИС с необходимыми доступы. После этого администратор ДИТ/ДЦТ предоставляет работнику необходимый доступ в ИС Университета и в Заявке отмечает исполнение. После этого заявка закрывается.

2.3 Для нового преподавателя предоставление Логина и Пароля осуществляется в автоматическом режиме в системе Фронт. Для этого после прохождения ККК и выхода Приказа о приеме на работу ответственный работник ДЧРиД подтверждает нового преподавателя в системе Фронт, и преподаватель автоматически получает Логин и Пароль на личную почту, которая им была указана при регистрации в системе Фронт. Так же ответственный работник ДЧРиД оформляет Заявку (форму прием на работу) в системе GLPI на предоставление доступов новому работнику. В заявке указываются необходимые данные согласно форме и вкладывается скан Приказа о приеме на работу. После этого администратор ДИТ предоставляет доступ преподавателю к стандартным ИС Университета. После этого заявка закрывается.

2.4 Для нового студента предоставление Логина и Пароля осуществляется в автоматическом режиме в системе Фронт. Для этого после заполнения всех данных о студенте в системе Фронт и после выхода Приказа о зачислении ответственный работник ДАВ подтверждает нового студента в системе Фронт, и студент автоматически получает Логин и Пароль на личную почту, которая им была указана при регистрации в системе Фронт.

2.5 Пользователь после получения Логина и первоначального Пароля обязан после первой регистрации сменить пароль через служебный компьютер или через систему Фронт. И для повторного входа в систему использовать свой уникальный Пароль согласно требованиям Парольной политике Университета.

2.6 Пользователь обязан производить смену пароля во всех ИС в соответствии с парольной политикой Университета. Система автоматический оповещает о необходимости смены пароля, после чего пользователь должен незамедлительно сменить пароль.

2.7 Пользователь обязан выключать РС или производить блокирование рабочей станции, средствами установленной операционной системы на РС, на время своего отсутствия на рабочем месте. На РС работниками ДИТ должна быть настроена и включена функция автоматического блокирования экрана после бездействия системы более 7 (семи) минут для работников Университета и 15 (пятнадцать) минут для всех остальных пользователей Университета.

2.8 В случае выявления пользователем возможности подключения к ИС, к которым ему не предоставлены права доступа согласно выполняемым должностным обязанностям, он не должен пытаться подключиться к данной ИС, Такие подключения рассматриваются - как попытки несанкционированного доступа к ИС и к пользователям принимаются меры в соответствии с главой 5 настоящих Правил.

2.9 В случае автоматической блокировки доступа и выявления фактов несанкционированного доступа к ИС со стороны третьих лиц, компрометации

(разглашения) пароля и т.д., пользователь обязан незамедлительно сообщить об этом факте в ДИТ всеми доступными методами (по телефону, почтой, сообщением в мессенджере) и завести Заявку в системе регистрации инцидентов GLPI с указанием сути инцидента и объяснением его возможных причин. Администраторы ДИТ и ДЦТ производят подключение/отключение доступов согласно распорядительных и внутренних нормативных документов Университета, регламентирующих предоставления доступов к ИС.

2.10 Во время нахождения работника в отпуске, командировке, на больничном и/или на учебе учётная запись пользователя должна быть временно заблокирована согласно распорядительным и внутренним нормативным документам Университета, регламентирующим порядок предоставления доступов к ИС.

2.11 Процедура разблокировки доступа пользователя к ИС производится согласно внутренним нормативным документам Университета, регламентирующим порядок предоставления доступов к ИС.

3. Порядок использования Информационных систем

3.1 Пользователю запрещается:

1) использовать пароль, предоставленный администратором для первоначального доступа к ИС, в качестве постоянного рабочего пароля;

2) передавать свои учетные записи и пароли третьим лицам (в связи с отпуском, командировкой и т.п.). Основанием для использования чужой учётной записи является Приказ о возложении обязанностей или Приказ о совмещении обязанностей, подписанная скан-копия которого должна предоставляться ДЧРиД в ДИТ не менее чем за 1 (один) рабочий день до возложения или совмещения обязанностей на работника. При отсутствии работника по причине болезни и в случае необходимости использования его учетной записи для исполнения рабочего процесса руководитель СП или лицо его замещающее направляет Заявку по системе GLPI в ДИТ с объяснением необходимости временного использования учетной записи заболевшего работника и указанием ФИО замещающего работника, кому передается его учетная запись. Подключение и отключение доступов производится согласно внутренним нормативным документам Университета, регламентирующим порядок предоставления доступов к ИС;

3) хранить пароль на любых носителях (бумажных или электронных – например, в ежедневниках, файлах или флэш/дисках), позволяющих другим лицам получить информацию о пароле. Оставлять данные об учетных записях в ИС на видных местах (например – монитор, клавиатура, системный блок, телефонный аппарат и т.п.);

4) несанкционированный доступ к информации, расположенной на прочих компьютерах и серверах сети Университета;

5) повреждение, уничтожение или фальсификация чужой информации;

6) использование и распространение информации, запрещенной действующим законодательством Республики Казахстан, внутренними нормативными документами Университета, а также противоречащей общепринятым морально-этическим нормам;

7) самостоятельное подключение компьютерного и прочего оборудования к сети Университета;

8) использование ресурсов ИС и корпоративной сети Университета в неслужебных целях (например - передаче и хранении личных фотографий, фильмов, файлов и прочее);

9) использовать информацию, полученную в результате доступа к корпоративной сети и ИС, в целях, не предусмотренных его функциональными и должностными обязанностями и технологическими схемами;

10) самостоятельно устанавливать или удалять аппаратное или программное обеспечение, а также вносить изменения в системную конфигурацию микропрограммного обеспечения базовой системы ввода-вывода BIOS (basic input/output system) компьютерного оборудования;

11) вскрывать компьютерную технику Университета;

12) без согласования с ДИТ предоставлять доступ к РС (самовольно предоставлять доступ по сети к дискам или папкам компьютера, предоставлять РС для работы других пользователей), сторонним лицам и организациям в любой форме, либо другим работникам. Использовать ПО предоставляющие сервисы удалённого доступа (Radmin, TeamViever AnyDesk - программы удаленного управления и администрирования компьютера через корпоративную сеть или интернет) и портативные версии приложений (например - папки общего доступа) для предоставления удаленного доступа к РС пользователя и ИС Университета;

13) копирование информации, как на внешние носители, так и с внешних носителей любых типов даже при наличии технической возможности без санкции ДИТ, кроме случаев регламентируемых внутренними нормативными и/или распорядительными документами Университета и необходимостью выполнения должностных обязанностей пользователя (например – запись рекламной продукции в Департаменте маркетинга).

3.2 В случае обнаружения случаев некорректной работы программного обеспечения, о программных сбоях и технических неполадках в ИС и отдельных компьютерах пользователи ставят в известность администраторов ДИТ (аналогично пункту 2.9). ДИТ имеет право на проведение запланированных и выборочных проверок ПО на рабочих станциях/серверах пользователей.

3.3 При работе с ИС и ПО пользователь должен руководствоваться только соответствующими внутренними нормативными документами Университета, а также письменными и устными рекомендациями работников ДИТ.

3.4 Вынос любого оборудования с территории, внос на территорию или перемещение по помещениям Университета осуществляется по согласованию с ДИТ согласно требованиям внутренних нормативных документов Университета, регламентирующим данный порядок.

3.5 Пользователи обязаны без промедления выполнять указания администраторов ДИТ в части использования компьютерной техники. Предоставлять доступ к своим рабочим станциям работникам ДИТ в случаях, плановых и не плановых проверок, технической необходимости, проведения технического обслуживания, эпидемий компьютерных вирусов, либо появления других случаев и обстоятельств, критичных для функционирования информационных систем. При технической необходимости и эпидемиях компьютерных вирусов администраторы ДИТ делают информационную рассылку по системе внутреннего документооборота Университета.

3.6 При обнаружении нарушений пользователем требований настоящих Правил, администраторы ДИТ действуют согласно Главе 5 настоящих Правил.

4. Ответственность пользователей корпоративной сети

4.1 Ответственность за сохранность и правильное использование информации, полученной из ИС, находящейся на компьютере пользователя, несет пользователь,

имеющий доступ к ИС, и руководитель СП, в составе которого работает пользователь. При приёме на работу новый работник должен проходить инструктаж в ДЧРиКР и должен быть предупреждён об ответственности выполнения настоящих Правил под роспись.

4.2 Пользователь несет личную ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования учетной записи.

4.3 Ответственность за соблюдение требований, указанных в Правилах, несут работник и руководитель СП, в рамках своей компетенции.

4.4 Ответственность за соблюдение сроков и требований, указанных в Правилах, несут соответствующие администраторы ДИТ/ДЦТ в рамках их компетенции.

5. Порядок отключения пользователя от корпоративной сети

5.1 При однократном нарушении (в течение года) требований настоящих Правил, не приведшем к нарушениям безопасности и работоспособности сети, пользователь получает предупреждение. Предупреждение может быть в любой форме: устно по телефону, письменно - в виде предупреждения по почтовой системе. Предупреждение может быть направлено непосредственному руководителю СП от администратора ДИТ.

5.2 При неоднократном (два и более раза в течение года) нарушении требований настоящих Правил или в случае, если нарушение привело к сбоям в работе сети, потере, модификации или раскрытию конфиденциальной информации, компьютер и учетная запись пользователя отключаются администраторами ДИТ и ДЦТ от корпоративной сети. Информация о данном факте отправляется ДИТ аналогично пункту 5.1. настоящих Правил с обязательным извещением об инциденте руководителя СП пользователя и Проректора по Цифровизации. Дальнейшие действия ДИТ осуществляются согласно внутренним нормативным документам Университета, регламентирующим процедуру проведения служебного расследования. На время проведения расследования учетная запись пользователя должна быть заблокирована.

5.3 При увольнении пользователь должен быть отключен от корпоративной сети Университета. Для этого ответственный работник ДЧРиД оформляет Заявку (форму увольнения) в системе GLPI на отключение доступов увольняющемуся пользователю. В заявке указываются необходимые данные согласно форме и вкладывается скан Приказа об увольнении. После этого администраторы ДИТ и ДЦТ отключают все доступы к ИС Университета. После этого заявка закрывается.

6. Заключительные положения

6.1 Правила обязательны для соблюдения всеми пользователями корпоративной сети Университета.

6.2 Контроль над надлежащим исполнением и соблюдением требований настоящих Правил осуществляют ответственные работники ДИТ.

6.3 Контроль над реализацией данных Правил, совершенствованием системы администрирования паролей и действиями администраторов ДИТ/ДЦТ и директора ДИТ возлагается на Проректора по Цифровизации.

6.4 Данные Правила вступают в силу с момента ее утверждения и подписания Ученым советом УМБ.