ПРАВИЛА
РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА К ЭЛЕКТРОННЫМ РЕСУРСАМ

Астана
2023 г.

1. Термины и сокращения

Организация – ОЮЛ Ассоциация ВИЭ «Qazaq Green»;

Правила – Правила разграничения прав доступа к электронным ресурсам;

Специалист по информационной безопасности – сотрудник Организации, ответственный за обеспечение защиты информационных ресурсов и обеспечение информационной безопасности Организации;

Системный администратор (далее – СА) – работник, который выполняет функции администрирования серверов и прикладного активного оборудования корпоративной информационной сети, и (или) отвечающий за администрирование:

- информационных систем Организации;
- серверов баз данных сопровождаемых ИС.

Специалист отдела кадров – работник по управлению персоналом либо лицо, исполняющее его обязанности и/или функции.

2. Общие положения

1. Настоящие Правила регламентируют доступ к информационным, программным и аппаратным ресурсам, организационно-техническое обеспечение процесса регистрации пользователей персональных компьютеров и системных администраторов ИС, удаление учетных записей в Организации.

2. Организационное и техническое обеспечение процесса доступа к информационным, программным и аппаратным ресурсам пользователей возлагается на системного администратора.

3. Правила регистрации пользователей

3. При поступлении на работу нового сотрудника специалист отдела кадров Организации в соответствии со служебными обязанностями сотрудника подает специалисту по информационной безопасности заявку, оформленную в виде служебной записки, о предоставлении необходимого доступа к информационным ресурсам для выполнения служебных обязанностей.

4. После оформления приема на работу нового сотрудника, специалист отдела кадров в соответствии с правилами ведения кадрового делопроизводства направляет специалисту по информационной безопасности заявку о необходимости подготовки рабочего места сотрудника, на основании которой производится регистрация пользователя (создание учетной записи пользователя) с предоставлением доступа к информационным ресурсам Организации.

5. Для некоторых сотрудников, в случае производственной необходимости допускается использование нескольких учетных записей.

6. Пароль должен отвечать требованиям Правила организации процедуры аутентификации Организации.

7. Требования к имени в сетевом окружении (hostname):

1) Имя в сетевом окружении определяется исходя из имени подразделения и имени сотрудника, разделенных символом нижнего подчеркивания.

2) В графу «Описание компьютера» вносится информация о пользователе (фамилия, имя) на русском языке, идентифицирующая пользователя в сетевом окружении.

8. После регистрации в сети пользователю для ознакомления предоставляются утвержденные правила и инструкции Организации по информационной безопасности.

9. Пользователь обязан руководствоваться правилами и инструкциями Организации по информационной безопасности.

10. СА предоставляет пользователям доступ к ресурсам в соответствии с утвержденными Правилами функционирования информационных систем.

11. СА обязан вести электронный журнал регистрации пользователей, содержащий следующие графы:

1) фамилия, имя, отчество;
2) подразделение;
3) должность;
4) адрес, телефон;
5) адрес электронной почты;
6) наличие Интернет;
7) название персонального компьютера в сетевом окружении (hostname);
8) доступ к сетевым дискам;
9) уровни доступа.

12. При увольнении сотрудника Организации, СА, прежде чем поставить отметку в обходном листе, обязан блокировать учетную запись пользователя в сети, и удалить её по истечению трех лет.

13. При переводе пользователя СА должен внести соответствующие изменения в профиль пользователя и журнал регистрации пользователей.

4. Основные права, обязанности и ответственность

14. Обязанности по предоставлению и аннулированию доступа к Ресурсам возлагаются на системного администратора Организации в

соответствии с положениями об отделах и должностными регламентами сотрудников.

15. Обязанности по контролю соблюдения Правил возлагаются на Специалиста по информационной безопасности Организации.

16. Пользователи допускаются к работе с ресурсами только после ознакомления под роспись в соответствующем журнале (**Приложение 1**, далее – Журнал инструктажа пользователей) с положениями Правил и прохождения инструктажа, проводимого Специалистом по информационной безопасности.

17. Соблюдение требований Правил обязательно для всех пользователей, допущенных к работе с ресурсами.

18. Дополнительно к настоящим Правилам допуск специалистов внешних организаций к выполнению работ на территории Организации регламентируется соответствующим нормативным документом Организации.

19. Деятельность пользователей при работе с ресурсами может протоколироваться и периодически проверяться на предмет соблюдения установленных правил работы любыми средствами, не противоречащими законодательству Республики Казахстан.

5. Учет ресурсов

20. Все информационные ресурсы Организации должны быть учтены и систематизированы в соответствующем Реестре.

21. Ведение Реестра возлагается на системного администратора Организации.

22. Актуальный Реестр должен быть доступен всем пользователям в произвольный момент времени.

23. Информация о новом ресурсе (изменениях в имеющемся ресурсе) должна быть доведена подразделением – владельцем ресурса до Специалиста по информационной безопасности Организации в течение двух рабочих дней с момента появления в виде служебной записки, подписанной системным администратором (**Приложение 2**).

24. Внесение изменений в Реестр осуществляется в течение одного рабочего дня с момента поступления соответствующей служебной записки.

6. Предоставление доступа к ресурсам

25. Для предоставления доступа пользователю к ресурсу необходимо выполнение одного из следующих условий:

- доступ необходим для выполнения пользователем должностных обязанностей в соответствии со своим должностным регламентом;

- доступ необходим для выполнения пользователем обязанностей другого пользователя по поручению (в виде служебной записки) системного администратора;

- доступ необходим для выполнения пользователем обязанностей другого пользователя по указанию (в виде приказа или распоряжения) руководства Организации;

- доступ необходим для выполнения пользователем работ по указанию (в виде приказа или распоряжения) руководства Организации;

- доступ необходим для выполнения пользователем работ в ходе реализации контрактов, договоров, заключенных Организацией (для сотрудников «сторонних» организаций).

26. Для обеспечения доступа к ресурсам системный администратор Организации (лицо, его замещающее) составляет заявку на предоставление доступа (далее – Заявка, **Приложение 3**), руководствуясь Реестром.

27. Системный администратор Организации в течение одного рабочего дня проверяет наличие у пользователя основания на доступ к ресурсу согласно Заявке. В случае если доступ к ресурсу согласно Заявке по какой-либо причине не может быть предоставлен, Заявка возвращается руководителю подразделения, инициировавшему Заявку, с подробным описанием данной причины.

28. После согласования с Специалистом по информационной безопасности Заявка передается на утверждение руководителю Организации (лицу, его замещающему). В случае утверждения в тот же день оригинал утвержденной Заявки передается специалисту по информационной безопасности на постоянное хранение, а копия Заявки (с указанным номером Заявки) – системного администратору для выполнения работ по предоставлению доступа согласно Заявке.

29. Информация об утвержденных Заявках заносится в журнал регистрации и учета заявок на предоставление доступа к ресурсам (далее – Журнал регистрации заявок, **Приложение 4**), который ведется в электронном виде системным администратором.

30. Для получения доступа к сетевым ресурсам необходима авторизация в Active Directory.

31. Контроль предоставления доступа осуществляется системным администратором.

32. Пользователи, авторизованные в Active Directory, имеют доступ к корпоративной почте, системе электронного документооборота.

33. Уровни доступа представлены в матрице доступа.

34.Для подключения к ИС используется VPN-соединение (SSTP, протокол https), внутри VPN-туннеля используется https, порт 81.

7. Использование ресурсов

35. Использование ресурсов осуществляется в соответствии с инструкциями по эксплуатации к программному и аппаратному обеспечению.

36. Запрещается умышленное выведение ресурсов из строя, блокировка доступа к ним и любые иные действия, препятствующие штатному режиму эксплуатации ресурсов.

37. В случае обнаружения сбоя в работе ресурса пользователь обязан сообщить об инциденте системного администратора и специалиста по информационной безопасности.

8. Изменение прав доступа к ресурсам

38. В случае необходимости предоставления пользователю дополнительных полномочий (ролей) по доступу к уже используемому им ресурсу следует действовать в соответствии с разделом 6 Правил.

39. В случае необходимости замены (полной или частичной) полномочий пользователя по доступу к уже используемому им ресурсу следует действовать в соответствии с п.40 Правил.

7. Аннулирование доступа к ресурсам

40. Аннулирование доступа к ресурсам происходит в случаях:

- изменения должностных обязанностей пользователя;
- истечения периода действия Заявки;
- изменения технологических процессов обработки информации таким образом, что доступ пользователю более не требуется;
- нарушения пользователем правил доступа к ресурсу;
- ухода сотрудника в декретный отпуск (отпуск по уходу за ребенком);
- увольнение пользователя;
- по иным требованиям руководства Организации или системного администратора Организации.

Аннулирование доступа должно быть инициировано в течение одного рабочего дня с момента возникновения соответствующего события.

41. Обязанности по инициированию аннулирования доступа пользователя к ресурсам возлагаются:

- в случае изменения должностных обязанностей пользователя или его увольнения, изменения технологических процессов обработки информации

таким образом, что доступ пользователю более не требуется - на системного администратора Организации;

- в случае истечения периода действия Заявки, нарушения пользователем правил доступа к ресурсу – на Специалиста по информационной безопасности Организации.

42. Информация об инициировании аннулировании доступа (с указанием причины) доводится в произвольной форме в письменном виде руководителем соответствующего подразделения Организации до Специалиста по информационной безопасности.

43. Аннулирование доступа осуществляется системным администратором по указанию Специалиста по информационной безопасности

44. Информация об аннулировании доступа заносится Специалистом по информационной безопасности в течение одного рабочего дня в Журнал регистрации заявок.

8. Контроль над соблюдением Правил

45. Специалист по информационной безопасности раз в полугодие проверяет соответствие перечня зарегистрированных пользователей штатному расписанию и его изменениям, и предоставляет отчет первому руководителю в рамках внутреннего аудита.

46. За нарушения норм, предусмотренных настоящими Правилами, к работникам Организации по представлению руководителя, курирующего вопросы информационной безопасности, на основании материалов служебного расследования, могут быть применены меры дисциплинарного взыскания.

9. Рассылка

С данным документом под роспись должны быть ознакомлены все сотрудники Организации (далее – Лист ознакомления).

Приложение 1
к Правилам разграничения прав доступа
к электронным ресурсам
«__» _____ 202_ г. № __

Журнал

инструктажа пользователей с правилами доступа к ресурсам ОЮЛ Ассоциация ВИЭ «Qazaq Green»

№ п/п	Инструктаж получил:			Инструктаж провел:		
	Фамилия И.О.	Занимаемая должность	Подпись	Фамилия И.О.	Подпись	Дата

Специалист по информационной безопасности

_____

(Ф.И.О.)

Приложение 2
к Правилам разграничения прав
доступа к электронным ресурсам
«__» _____ 202_ г. № __

СЛУЖЕБНАЯ ЗАПИСКА

В соответствии с Правилами разграничения прав доступа к информационным ресурсам, утвержденным приказом от «____»_____.202__г. № _____, прошу включить (аннулировать) в (из) реестр(а) новый информационный ресурс.

Наименование информационного (программного) ресурса	Основание для включения нового ресурса в реестр организации (дата и номер закона либо другого нормативного акта)	Период действия (постоянно или указать интервал)
1	3	6

Системный администратор _____

«____» _____202__г _____
подпись

Приложение 3
к Правилам разграничения прав доступа
к электронным ресурсам
«__» _____ 202_ г. № __

Заявка №____
на предоставление доступа к информационным, программным и аппаратным ресурсам
ОЮЛ Ассоциация ВИЭ «Qazaq Green»

Фамилия И.О. сотрудника, (таб.номер), должность	№ каб., Телефон (вн.)	Обоснование необходимости проведения указанного вида работ в соответствии с должностными обязанностями сотрудника (ссылка на раздел должностного регламента или иной нормативный документ в соответствии с п.4.1. Правил)	Ресурс (согласно Перечню)	Режим доступа (**открыть/закрыть**: чт/зап; просмотр, ввод, корр., распеч.)	Период действия (постоянно или указать интервал дат)
1	2	3	4	5	6

Системный администратор_____
«____» _____202___г _____
подпись

Приложение 4
к Правилам разграничения прав доступа
к электронным ресурсам
«__» _____ 202_ г. № __

Журнал
регистрации и учета заявок на предоставление доступа к информационным, программным и аппаратным ресурсам ОЮЛ Ассоциация ВИЭ «Qazaq Green»

Заявка №	ФИО, должность	Отдел	Информационный ресурс по заявке	Дата согласования заявки	Период доступа

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Личная подпись	Дата
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				