Закрытое акционерное общество
«Водород»

УТВЕРЖДЕНО
Приказом директора
ЗАО «Водород»
от 09.02.2022 № 4
(в редакции приказа ЗАО «Водород»
от 25.01.2023 № 6)

ПОЛОЖЕНИЕ
09.02.2022 № 02-03-05/5

г. Минск

о конфиденциальной информации
ЗАО «Водород»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Положение о конфиденциальной информации ЗАО «Водород» (далее – Положение) определяет правовые, организационные и технические основы режима конфиденциальности, порядок отнесения сведений к конфиденциальной информации, порядок доступа к конфиденциальной информации, порядок обращения носителей конфиденциальной информации, обязанности лиц, допущенных к конфиденциальной информации, порядок осуществления контроля выполнения требований режима конфиденциальности, ответственность за нарушение режима конфиденциальности, а также иные вопросы, касающиеся конфиденциальности информации.

2. Настоящее Положение разработано на основании Закона Республики Беларусь от 05.01.2013 № 16-З «О коммерческой тайне», Закона Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации», Закона Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» (далее – Закон о защите персональных данных), постановления Совета Министров Республики Беларусь от 12.08.2014 № 783 «О служебной информации ограниченного распространения», Положением о конфиденциальной информации ОАО «БПС-Сбербанк» от 22.01.2018 № 01/01 07/18, иных актов законодательства, локальных правовых актов (далее – ЛПА) и других документов ЗАО «Водород» (далее – Общество), регламентирующих правоотношения в сфере, обработки и защиты конфиденциальной информации, персональных данных, а также обеспечения информационной и кибербезопасности.

3. В случае изменения законодательства, регулирующего вопросы ограничения доступа к сведениям, в период до внесения соответствующих

изменений и/или дополнений в настоящее Положение, оно применяется в части, не противоречащей законодательству.

4. Для целей настоящего Положения используются следующие термины и их определения:

банковская тайна – сведения о счетах и вкладах (депозитах), в том числе о наличии счета в банке (небанковской кредитно-финансовой организации), его владельце, номере и других реквизитах счета, размере средств, находящихся на счетах и во вкладах (депозитах), а равно сведения о конкретных сделках, об операциях без открытия счета, операциях по счетам и вкладам (депозитам), а также об имуществе, находящемся на хранении в банке;

владелец конфиденциальной информации – юридическое или физическое лицо, в том числе индивидуальный предприниматель, а также государственный орган, организация, в том числе не являющаяся юридическим лицом, правомерно обладающие сведениями, в отношении которых такими лицами установлен режим конфиденциальности, за исключением случаев, когда эти сведения составляют конфиденциальную информацию других лиц;

гриф ограничения доступа – реквизит, проставляемый на носителе конфиденциальной информации и/или сопроводительной документации к нему, свидетельствующий о наличии на этом носителе конфиденциальной информации;

доступ к конфиденциальной информации – возможность ознакомления с согласия владельца конфиденциальной информации или на ином законном основании определенного круга лиц со сведениями, содержащими конфиденциальную информацию;

запоминающее устройство – носитель информации, установленный в системный блок или подключаемый к персональному компьютеру, серверу, иному техническому средству накопления, хранения и обработки информации в цифровом виде;

защита конфиденциальной информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности конфиденциальной информации;

коммерческая тайна – сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), соответствующие требованиям Закона о коммерческой тайне, в отношении которых установлен режим конфиденциальности;

контрагент – лицо, с которым у Общества имеется действующий гражданско-правовой договор на проведение работ (оказание услуг); не являются контрагентами лица, состоящие с Обществом в трудовых отношениях;

конфиденциальная информация – служебная информация ограниченного распространения; сведения, составляющие банковскую тайну; коммерческая

тайна ОАО «Сбер Банк» (далее – Банк) или Общества; конфиденциальная информация третьих лиц, доступ к которой ограничен ими на законном основании, обозначенная как конфиденциальная информация (путем присвоения грифа ограничения доступа или иным способом), к которой Общество получило доступ; информация о частной жизни физических лиц и персональные данные; иные сведения, доступ к которым ограничен в соответствии с законодательством Республики Беларусь;

конфиденциальность информации – требование не допускать разглашения, распространения и/или предоставления конфиденциальной информации без согласия ее владельца или иного основания, предусмотренного законодательными актами Республики Беларусь;

личный ключ электронной цифровой подписи – последовательность символов, принадлежащая определенной организации или физическому лицу и используемая при выработке электронной цифровой подписи;

носитель конфиденциальной информации – документ или иной материальный объект, на котором сведения, содержащие конфиденциальную информацию, содержатся в любой объективной форме, в том числе в виде символов, образов, сигналов, позволяющих эти сведения распознать и идентифицировать;

обязательство о неразглашении конфиденциальной информации – гражданско-правовой договор, заключаемый владельцем конфиденциальной информации или лицом, получившим к ней доступ, с лицом, состоящим в трудовых отношениях с владельцем конфиденциальной информации или лицом, получившим к ней доступ, и определяющий обязательства сторон, связанные с соблюдением конфиденциальности сведений, доступ к которым ограничен на законном основании;

персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано, в соответствии с Законом о защите персональных данных;

предоставление конфиденциальной информации – действия, направленные на ознакомление с конфиденциальной информацией определенного круга лиц;

разглашение конфиденциальной информации – действия (бездействие), в результате которых сведения, содержащие конфиденциальную информацию, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становятся известными третьим лицам без согласия владельца конфиденциальной информации или иного законного основания;

распространение конфиденциальной информации – действия, направленные на ознакомление с конфиденциальной информацией неопределенного круга лиц;

режим конфиденциальности – правовые, организационные, технические и иные меры, принимаемые в целях обеспечения конфиденциальности сведений, доступ к которым ограничен на законном основании;

служебная информация ограниченного распространения – сведения, касающиеся деятельности государственного органа, юридического лица, распространение и/или предоставление которых могут причинить вред национальной безопасности Республики Беларусь, общественному порядку, нравственности, правам, свободам и законным интересам физических лиц, в том числе их чести и достоинству, личной и семейной жизни, а также правам и законным интересам юридических лиц и которые не отнесены к государственным секретам;

соглашение о конфиденциальности – гражданско-правовой договор, заключаемый владельцем конфиденциальной информации с контрагентом, предметом которого являются обязательства сторон по обеспечению конфиденциальности сведений, содержащих конфиденциальную информацию;

средства защиты конфиденциальной информации – технические, программные, криптографические и другие средства, используемые для защиты конфиденциальной информации, а также средства контроля эффективности защиты конфиденциальной информации;

структурные подразделения Общества – самостоятельные отделы или другие подразделения Общества;

физическое лицо, которое может быть идентифицировано, – физическое лицо, которое может быть прямо или косвенно определено, в частности через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности;

электронная цифровая подпись – последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности.

ГЛАВА 2
РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ

5. Правовую основу режима конфиденциальности составляют правовые акты, указанные в пункте 2 настоящего Положения, а также настоящее Положение.

6. Организационную и техническую основу режима конфиденциальности составляют:

установление порядка отнесения сведений к конфиденциальной информации;

установление порядка доступа к конфиденциальной информации;

установление порядка обращения с носителями конфиденциальной информации;

организация учета и определение обязанностей лиц, допущенных к конфиденциальной информации;

установление порядка осуществления контроля выполнения требований режима конфиденциальности;

ответственность за нарушение режима конфиденциальности и/или разглашение конфиденциальной информации;

организация технической и/или криптографической защиты конфиденциальной информации, контроль защищенности конфиденциальной информации, выявление и контроль возможных каналов ее утечки.

ГЛАВА 3
ПОРЯДОК ОТНЕСЕНИЯ СВЕДЕНИЙ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, УСТАНОВЛЕНИЯ, ИЗМЕНЕНИЯ И ОТМЕНЫ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ

7. Сведения, содержащие конфиденциальную информацию, в отношении которых устанавливается режим конфиденциальности, включаются в Перечень конфиденциальной информации ЗАО «Водород» (Приложение 1 к настоящему Положению) (далее – Перечень).

Отнесение сведений к конфиденциальной информации осуществляется на основании Перечня.

8. В Перечень включаются:

сведения, отнесенные в соответствии с Постановлением о служебной информации к служебной информации ограниченного распространения;

сведения, составляющие в соответствии со статьей 121 Банковского кодекса Республики Беларусь банковскую тайну;

сведения, составляющие коммерческую тайну Банка или Общества в соответствии с настоящим Положением;

персональные данные;

конфиденциальные сведения третьих лиц, на законном основании ограниченные ими к распространению и обозначенные как конфиденциальные сведения (путем присвоения грифа ограничения доступа или иным способом), к которым Общество получило доступ;

иные сведения, ограниченные к распространению в соответствии с законодательством Республики Беларусь.

9. Перечень обновляется по мере необходимости, но не реже 1 раза в 5 лет.

10. Включение сведений в Перечень и установление в отношении них режима конфиденциальности осуществляются по предложениям структурных подразделений Общества, подготовленным в соответствии с законодательством Республики Беларусь, регламентирующим вопросы ограничения доступа к сведениям, с обязательным соблюдением возложенных на Общество обязательств по действующим договорам (соглашениям).

Предложение оформляется в виде докладной записки на имя директора Общества (лица, исполняющего его обязанности), подписанной руководителем структурного подразделения Общества и согласованной с отделом безопасности Общества, а также ИТ-директором (для структурных

подразделений блока разработки) или заместителем директора по сопровождению (для структурных подразделений блока сопровождения).

Работники Общества, принявшие решение об отнесении сведений к конфиденциальной информации и проставлении на носителях конфиденциальной информации грифа ограничения доступа, несут персональную ответственность за обоснованность принятого решения;

11. Внесение изменений и/или дополнений в Перечень, в том числе исключение из него сведений, изменение или отмена в отношении них режима конфиденциальности осуществляются в установленном порядке по предложениям структурных подразделений Общества, подготовленным и оформленным в порядке, предусмотренном пунктом 9 настоящего Положения.

12. Изменение (отмена) режима конфиденциальности в отношении сведений производится:

при изменении законодательства Республики Беларусь в части, устанавливающей ограничение распространения отдельных видов информации;

по истечении установленного Перечнем срока действия режима конфиденциальности в отношении сведений;

при внесении изменений в Перечень, в том числе исключения из него сведений;

при изменении (отмене) режима конфиденциальности владельцем конфиденциальных сведений, к которым Общество получило доступ, подтвержденного в письменной форме;

при установлении необоснованности отнесения сведений к конфиденциальной информации.

13. Отметка о снятии грифа ограничения доступа с носителей конфиденциальной информации производится работником, в чьем производстве находится данный документ.

ГЛАВА 4
ПОРЯДОК ДОСТУПА РАБОТНИКОВ ОБЩЕСТВА К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

14. Все работники Общества подписывают обязательство о неразглашении конфиденциальной информации (Приложение 2 к настоящему Положению).

Обязательство о неразглашении конфиденциальной информации дается в письменной или электронной форме. Электронная форма обязательства о неразглашении конфиденциальной информации удостоверяется электронной цифровой подписью с использованием личного ключа электронной цифровой подписи работника.

15. Доступ к конфиденциальной информации, в том числе доступ к информационным ресурсам, содержащим конфиденциальную информацию, работники Общества получают на основании приказа о назначении на

должность, после подписания обязательства о неразглашении конфиденциальной информации и изучения законодательства Республики Беларусь, ЛПА Общества и иных документов, регламентирующих вопросы ограничения доступа к сведениям, в объеме, необходимом и достаточном для качественного исполнения ими своих служебных обязанностей в части, касающейся конфиденциальности информации.

16. Обязанность по ознакомлению работника с законодательством Республики Беларусь, ЛПА Общества и иными документами, регламентирующими вопросы ограничения доступа к сведениям, возлагается на отдел управления персоналом (при трудоустройстве нового работника), а также на руководителя соответствующего структурного подразделения.

Руководитель структурного подразделения обязан создать условия и обеспечить доступ к конфиденциальной информации только в том объеме, который необходим работнику для выполнения своих должностных обязанностей.

17. К работе с конфиденциальной информацией допускаются работники Общества, имеющие к ней непосредственное отношение, в соответствии с должностными обязанностями или согласно указаниям, содержащимся в резолюциях руководителей.

18. Доступ к информационным ресурсам, содержащим конфиденциальную информацию, осуществляется в соответствии с требованиями ЛПА в сфере информационной безопасности и кибербезопасности.

19. В целях исключения несанкционированной утечки конфиденциальной информации в служебных помещениях Общества запрещается использование технических средств (мобильные телефоны, фотоаппараты, планшеты, диктофоны и т.п.) для осуществления аудио-, фото- и видеофиксации такой информации.

Разрешение на аудио-, фото-, видеофиксацию конфиденциальной информации при наличии на такие действия предварительного согласия одела безопасности Общества дает директор Общества (лицо, исполняющее его обязанности).

ГЛАВА 5
ПОРЯДОК ДОСТУПА КОНТРАГЕНТОВ И ГОСУДАРСТВЕННЫХ ОРГАНОВ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

20. Для обеспечения доступа к конфиденциальной информации контрагентов с ними в письменной форме заключается самостоятельное соглашение о конфиденциальности (NDA) (типовая форма приведена в Приложении 3 к настоящему Положению) или в договор, для исполнения которого необходим доступ к конфиденциальной информации, включается раздел о конфиденциальности (типовая форма приведена в Приложении 4 к настоящему Положению).

По согласованию с отделом безопасности Общества допустимо, в том числе при поступлении мотивированного требования контрагента, заключение соглашения о конфиденциальности или включение в договор раздела о конфиденциальности по форме / в редакции, отличающихся от типовых форм, приведенных в Приложениях 4 и 5 к настоящему Положению.

21. Соглашение о конфиденциальности либо раздел о конфиденциальности в структуре иного договора в обязательном порядке должны содержать:

21.1. перечень сведений, составляющих конфиденциальную информацию, или порядок их определения;

21.2. пределы использования сведений, составляющих конфиденциальную информацию;

21.3. указание о сроке, в течение которого контрагент обязан обеспечить конфиденциальность сведений, составляющих конфиденциальную информацию, в том числе в случае досрочного расторжения договора или отказа от его исполнения;

21.4. обязательства сторон о неразглашении конфиденциальной информации и ответственность за ее разглашение.

22. Все заключаемые соглашения о конфиденциальности и договоры, содержащие раздел о конфиденциальности, до их подписания в обязательном порядке подлежат согласованию с отделом безопасности Общества.

23. Для обеспечения доступа контрагентов к информационным ресурсам Общества, содержащим конфиденциальную информацию, дополнительно устанавливаются правила информационной безопасности при работе в информационной системе Общества (типовая форма приведена в Приложении 5 к настоящему Положению), оформляемые, как правило, в виде приложения к соглашению о конфиденциальности, а при его отсутствии – к договору, для исполнения которого необходим доступ к конфиденциальной информации.

24. Доступ к конфиденциальной информации контрагентам предоставляется в объеме, необходимом и достаточном для исполнения сторонами обязательств по договору.

25. Решение, в каком объеме предоставляется доступ к конфиденциальной информации контрагентам, принимает руководитель структурного подразделения Общества, инициировавшего заключение договора с контрагентом, с учетом следующих особенностей:

25.1. доступ третьих лиц к сведениям, составляющим банковскую тайну, предоставляется с учетом требований статьи 121 Банковского кодекса Республики Беларусь на основании письменного согласия клиента Банка, являющегося владельцем конфиденциальной информации;

25.2. доступ к конфиденциальной информации третьих лиц, к которой Общество получило доступ, предоставляется на основании письменного разрешения этих лиц, если иное не оговорено в соглашении о конфиденциальности или соответствующем разделе о конфиденциальности договора.

26. Доступ к конфиденциальной информации государственным или другим компетентным органам представляется в соответствии с законодательством Республики Беларусь на основании письменных запросов (иных установленных законодательством документов) этих органов в объеме, указанном в запросе.

27. Доступ к коммерческой тайне третьих лиц, к которой Общество получило доступ, не предоставляется, если иное не предусмотрено законодательными актами или соглашением о конфиденциальности или разделом о конфиденциальности договора с этим лицом. При поступлении такого запроса в ответ предоставляется только информация о владельце коммерческой тайны.

ГЛАВА 6
ПОРЯДОК ОБРАЩЕНИЯ С НОСИТЕЛЯМИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

28. Прием и регистрация, контроль исполнения, подготовка к отправке и пересылка адресатам, учет, тиражирование и копирование, уничтожение носителей конфиденциальной информации, присвоение (снятие) им (с них) грифа ограничения доступа, а при необходимости списание в дела, проведение экспертизы научной и практической ценности, подготовка и передача их для архивного хранения осуществляются в установленном в Обществе порядке, в том числе с учетом требований Положения о порядке проставления ограничительного грифа «Для служебного пользования» и ведения делопроизводства по документам, содержащим служебную информацию ограниченного распространения, утвержденного Постановлением о служебной информации.

29. Носители конфиденциальной информации, включить которые в дела обычным порядком не представляется возможным (компакт-диски, накопители на USB-носителях или флэш-картах памяти и т.п.), вкладываются в конверт, который нумеруется как лист дела.

На конверте указываются гриф ограничения доступа и идентификационные признаки вложенного в него носителя конфиденциальной информации:

вид носителя;

регистрационный номер, присвоенный работником структурного подразделения Общества, ответственным за делопроизводство;

ID или серийный номер носителя информации, присвоенный изготовителем (при его наличии);

идентификационные признаки находящейся на нем информации (имена и размер каждого файла, а при количестве файлов более 15 допускается указывать общее количество файлов и их общий объем).

Уничтожение носителей конфиденциальной информации, а также черновых материалов (документов, файлов и т.д.), содержащих конфиденциальную информацию, осуществляется способом, исключающим

возможность ее восстановления (прочтения текста, восстановления файлов или его части и т.д.).

30. Носители конфиденциальной информации должны храниться в служебных помещениях в сейфах, надежно запираемых шкафах, хранилищах либо ящиках рабочего стола, исключающих доступ к носителям конфиденциальной информации сторонних лиц, их хищение, а также приведение в негодность или уничтожение носителей конфиденциальной информации и/или содержащейся на них информации.

31. Получение носителя конфиденциальной информации удостоверяется работником росписью в учетной форме (журнале), составленном в любой удобной для ведения в Обществе форме.

32. Выданные для работы носители конфиденциальной информации подлежат возврату работнику, ответственному за делопроизводство в тот же день. Прием носителя конфиденциальной информации удостоверяется работником, ответственным за делопроизводство росписью в учетной форме (журнале).

Отдельные носители конфиденциальной информации, по решению руководителя структурного подразделения Общества, могут выдаваться работником, ответственным за делопроизводство, исполнителям на весь срок, необходимый для выполнения задания, при условии выполнения исполнителем требований пункта 30 настоящего Положения.

33. Оборот носителей конфиденциальной информации (получение, отправка, изъятие из дел) производится только работником, ответственным за делопроизводство.

34. Запрещается выносить носители конфиденциальной информации, в том числе технические средства с запоминающими устройствами, содержащими конфиденциальную информацию, за пределы помещений Общества без соответствующего разрешения.

В необходимых случаях руководители структурных подразделений Общества или вышестоящие руководители могут разрешить вынос носителей конфиденциальной информации за пределы помещений Общества, в том числе при организации дистанционного режима работы, при работе в служебных помещениях Банка или при командировании работников в другие населенные пункты на срок более одного дня.

Разрешение на вынос носителей конфиденциальной информации за пределы помещений Общества оформляется в письменном виде с указанием адреса места дистанционной работы, структурного подразделения Банка или наименования и адреса сторонней организации (при командировании работника), в которых разрешена работа с носителями конфиденциальной информации.

35. Особенности обращения запоминающих устройств, содержащих конфиденциальную информацию, регламентируется установленными в Обществе правилами информационной и кибербезопасности.

ГЛАВА 7
ПОРЯДОК ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ОБОРОТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

36. Запрещается передавать конфиденциальную информацию с использованием незащищенных средств связи и передачи информации (электронная почта, радиосвязь, телефонные, в том числе факсимильные, линии связи и т.п.).

37. Оборот конфиденциальной информации в электронном виде осуществляется только посредством используемой в Обществе системы электронного документооборота.

38. Обмен конфиденциальной информацией в электронном виде между Обществом и Банком или ПАО Сбербанк осуществляется только по специально выделенным защищенным каналам передачи информации.

39. Электронные копии конфиденциальной информации могут быть перенесены на другие электронные носители только с письменного разрешения (резолюции) руководителя структурного подразделения Общества или вышестоящих руководителей. При этом на носителе проставляется гриф ограничения доступа и номер экземпляра. Носитель конфиденциальной информации регистрируется в учетной форме (журнале) работником, ответственным за делопроизводство, в чьем производстве находится данный документ.

40. Хранение конфиденциальной информации в электронном виде осуществляется на электронных носителях, а также на средствах вычислительной техники (в том числе в информационных системах, предназначенных для обработки конфиденциальной информации).

Хранение электронных носителей конфиденциальной информации осуществляется в условиях, исключающих доступ к носителям конфиденциальной информации сторонних лиц, возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

41. Для организации электронного оборота конфиденциальной информации с контрагентами в соответствии с требованиями законодательства Республики Беларусь создаются защищенные каналы связи.

В отдельных случаях, по согласованию с отделом безопасности Общества допускается передача по открытым каналам передачи данных файлов, защищенных (зашифрованных) средствами криптографической защиты (при их наличии). Возможность использования такого способа передачи конфиденциальной информации особо оговаривается сторонами в соглашении о конфиденциальности или разделе о конфиденциальности в договоре с контрагентом.

ГЛАВА 8
ПОРЯДОК ПРОВЕДЕНИЯ ЗАКРЫТЫХ СОВЕЩАНИЙ И ПЕРЕГОВОРОВ

42. Разрешение на проведение совещания (переговоров) по вопросам, содержащим конфиденциальную информацию, имеет право давать директор Общества (лицо, исполняющее его обязанности), а также в рамках курируемых направлений деятельности ИТ-директор, заместитель директора по сопровождению, финансовый директор или начальник отдела безопасности Общества.

43. Руководитель, давший разрешение на проведение совещания (переговоров) по вопросам, содержащим конфиденциальную информацию, назначает ответственного, который составляет список его участников с указанием их фамилии, имени и отчества (при его наличии), должности и наименования организации, а при необходимости и иных идентификационных признаков (личный номер, номер и дата документа, удостоверяющего личность и т.п.).

На совещание допускаются только лица, включенные в указанный список.

44. Совещание (переговоры) проводится в специально отведенном для этого помещении, проверенном на предмет возможной утечки информации по техническим или иным каналам и при необходимости оснащенном техническими средствами защиты от такой утечки.

45. Председательствующий на совещании (переговорах) обязан предупредить участников о неразглашении конфиденциальной информации, ответственности за ее разглашение и уточнить, какие сведения являются конфиденциальными.

По результатам совещания (переговоров) по вопросам, содержащим конфиденциальную информацию, в обязательном порядке оформляется протокол, в котором фиксируется факт предупреждения участников о неразглашении конфиденциальной информации и ответственности за ее разглашение, а также отражаются краткое содержание доклада/выступлений/прений и принятые решения.

ГЛАВА 9
ОБЯЗАННОСТИ РАБОТНИКОВ ОБЩЕСТВА, ДОПУЩЕННЫХ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

46. Руководители структурных подразделений Общества организуют и обеспечивают изучение подчиненными работниками нормативных правовых актов Республики Беларусь, ЛПА Общества, в том числе настоящего Положения, а также других документов, регламентирующих вопросы ограничения доступа к сведениям.

47. Работник Общества обязан:

47.1. знать и выполнять требования законодательства Республики Беларусь, ЛПА Общества, в том числе настоящего Положения, регламентирующих вопросы ограничения доступа к сведениям;

47.2. соблюдать требования установленного в Обществе режима конфиденциальности, не разглашать конфиденциальную информацию, к которой получил доступ в процессе служебной деятельности, третьим лицам,

а также другим работникам Общества, не имеющим отношения к этой информации;

47.3. выявлять причины и/или условия, создающие предпосылки для утечки конфиденциальной информации;

47.4. пресекать в силу своих возможностей и компетенций действия (бездействие) работников Общества, а также других лиц, которые могут привести к несанкционированному разглашению конфиденциальной информации;

47.5. не использовать сведения, ставшие известными в процессе служебной деятельности, в целях, не связанных с выполнением своих непосредственных должностных обязанностей;

47.6. не предоставлять третьим лицам, включая других работников Общества, выданные ему программно-технические средства и/или сведения (идентификаторы и пароли доступа, личный ключ электронной цифровой подписи и т.д.), необходимые для доступа к информационным ресурсам Общества;

47.7. выполнять только те работы и знакомиться только с теми материалами, которые предусмотрены его должностными обязанностями и к которым разрешен доступ;

47.8. принимать и передавать носители конфиденциальной информации только через работника, ответственного за ведение делопроизводства, под роспись, а в электронном виде – в порядке, предусмотренном главой 5 настоящего Положения;

47.9. при подготовке документов включать в их содержание минимально необходимую конфиденциальную информацию;

47.10. во время работы с носителями конфиденциальной информации принимать меры, исключающие возможность ознакомления с этой информацией лиц, не имеющих к ней отношения, включая других работников Общества (располагать документы соответствующим образом, при необходимости убирать или переворачивать их, скрывать конфиденциальную информацию, отображаемую на экране монитора, останавливать аудио- и/ил видео-воспроизведение конфиденциальной информации и т.д.);

47.11. предъявлять для проверки носители конфиденциальной информации по обоснованному требованию непосредственного руководителя, вышестоящих руководителей, работника, ответственного за делопроизводство, работников отдела безопасности Общества, а также других уполномоченных на проведение такой проверки работников Общества или Банка;

47.12. давать объяснения по выявленным фактам несанкционированного разглашения конфиденциальной информации, ее утраты или другого нарушения режима конфиденциальности, в том числе установленных правил обращения с носителями конфиденциальной информации;

47.13. незамедлительно, а при невозможности – в кратчайший срок проинформировать своего непосредственного руководителя и отдел безопасности Общества обо всех ставших известными ему:

47.13.1. фактах/обстоятельствах, указанных в подпунктах 47.3 и 47.4 настоящего пункта:

47.13.2. нарушениях режима конфиденциальности, в том числе установленных правил обращения с носителями конфиденциальной информации, разглашения (угрозы разглашения) конфиденциальной информации, незаконного ознакомления с конфиденциальной информацией, или незаконного использования конфиденциальной информации;

47.13.3. требованиях иных лиц предоставить им незаконный доступ к конфиденциальной информации, в том числе попытках этих лиц получить такой доступ под угрозой применения насилия или совершения иного противоправного действия, посредством обещания незаконного вознаграждения (материального либо путем предоставления услуги) и т.п.;

47.13.4. об утрате:

носителей конфиденциальной информации, в том числе отдельных листов документов, содержащих конфиденциальную информацию;

служебного удостоверения или постоянного (временного) пропуска;

личной печати;

ключей от служебных помещений, сейфовых комнат, сейфов (шкафов) и иных хранилищ, в которых хранятся носители конфиденциальной информации, в том числе электронных ключей доступа и электронных ключей управления роллетами;

программно-технических средств и сведений, необходимых для доступа к информационным ресурсам Общества, в том числе электронной цифровой подписи;

47.14. при увольнении, перед длительной командировкой, отпуском сдать работнику, ответственному за ведение делопроизводства, все имеющиеся у него носители конфиденциальной информации.

48. Работникам Общества запрещается:

48.1. сообщать конфиденциальную информацию в любой форме (устно, письменно и т.п.) третьим лицам, в том числе другим работникам Общества, не имеющим к ней прямого отношения;

48.2. размещать конфиденциальную информацию в сети Интернет или других общедоступных информационных ресурсах, а также передавать ее по незащищенным каналам связи;

48.3. использовать конфиденциальную информацию в целях, не связанных с выполнением своих непосредственных должностных обязанностей;

48.4. самостоятельно принимать от кого-либо или передавать кому-либо носители конфиденциальной информации;

48.5. при работе с носителями конфиденциальной информации, выходя из помещения, оставлять эти носители в свободном доступе, в том числе незапертом сейфе, ящике стола или другом хранилище, а также, при отсутствии в помещении других работников, оставлять незакрытыми двери и окна помещения, в котором хранятся носители конфиденциальной информации, что может повлечь несанкционированный доступ к ним

сторонних лиц, их хищение, приведение в негодность или уничтожение носителей конфиденциальной информации и/или содержащейся на них информации;

48.6. выносить за пределы помещений Общества носители конфиденциальной информации, в том числе технические средства с запоминающими устройствами, содержащими конфиденциальную информацию, без соответствующего разрешения;

48.7. предоставлять кому-либо, включая других работников Общества, выданные программно-технические средства и сведения, необходимые для доступа к информационным ресурсам Общества.

ГЛАВА 10
ПОРЯДОК ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ

49. Контроль выполнения требований режима конфиденциальности, в том числе с использованием средств мониторинга информации, циркулирующей в корпоративных сетях и средствах обработки информации (корпоративной телефонной сети, корпоративной локальной вычислительной сети, персональных компьютерах и т.д.), осуществляется с целью пресечения утечки конфиденциальной информации, оценки эффективности мер режима конфиденциальности, выявления недостатков и нарушений правил работы с носителями конфиденциальной информации, установления причин, способствующих появлению этих нарушений, выработки мер, направленных на их устранение.

50. Контроль выполнения требований режима конфиденциальности осуществляет отдел безопасности Общества.

51. Проверка выполнения требований режима конфиденциальности, организации работы с носителями конфиденциальной информации, их наличие проводится по указанию директора Общества (лица, исполняющего его обязанности) работником, ответственным за делопроизводство, или иным работником Общества, уполномоченным в установленном порядке на проведение такой проверки.

Периодичность проверки организации работы с носителями конфиденциальной информации и их наличия определяется директором Общества (лицом, исполняющим его обязанности), но не реже 1 раза в 3 года.

52. Проверяющий имеет право знакомиться с учетными формами и другими документами, а при выявлении недостатков и нарушений – требовать от работников предоставления соответствующих объяснений.

53. Результаты проверки докладываются докладной запиской на имя директора Общества (лица, исполняющего его обязанности), в которой дается оценка текущего состояния режима конфиденциальности в Обществе в целом или каком-то его структурном подразделении, отмечаются выявленные в процессе проверки недостатки и/или нарушения режима конфиденциальности, даются указания/рекомендации по их устранению,

указываются ответственные исполнители соответствующих мероприятий и сроки исполнения. При необходимости к докладной записке прилагаются иные материалы проверки.

О результатах выполнения мероприятий по устранению выявленных недостатков и/или нарушений режима конфиденциальности ответственный исполнитель докладывает директору Общества (лицу, исполняющему его обязанности) в установленном порядке.

54. О фактах разглашения (угрозы разглашения) конфиденциальной информации, в том числе утраты документов, дел, изданий, немедленно ставятся в известность директор Общества (лицо, исполняющее его обязанности), начальник отдела безопасности Общества, руководитель структурного подразделения Общества, в котором произошло разглашение (существует угроза разглашения) конфиденциальной информации, ИТ-директор или заместитель директора по сопровождению (соответственно для структурных подразделений блоков разработки или сопровождения), а также немедленно принимаются меры по устранению утечки информации и минимизации ущерба.

По фактам разглашения (угрозы разглашения) конфиденциальной информации, в том числе утраты документов, дел, изданий, содержащих конфиденциальную информацию, комиссией, назначаемой приказом директора Общества (лица, исполняющего его обязанности) проводится служебное разбирательство. Результаты служебного разбирательства докладываются директору Общества (лицу, исполняющему его обязанности).

По результатам служебного разбирательства комиссией разрабатывается комплекс мероприятий по устранению причин, вызвавших нарушение режима конфиденциальности, и минимизации причиненного ущерба, с указанием сроков исполнения и работников, ответственных за их исполнение.

О ходе выполнения мероприятий докладывается директору Общества (лицу, исполняющему его обязанности).

На утраченные носители конфиденциальной информации составляется акт, соответствующие отметки вносятся в учетные формы.

ГЛАВА 11
ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ

55. Ответственность за организацию и обеспечение режима конфиденциальности возлагается на директора Общества (лица, исполняющего его обязанности), ИТ-директора, заместителя директора по сопровождению, финансового директора, руководителей структурных подразделений Общества в пределах компетенции и по курируемым направлениям работы.

56. Работники Общества несут личную ответственность за нарушение режима конфиденциальности, разглашение конфиденциальной информации, утрату, незаконное уничтожение носителей конфиденциальной информации.

57. Работники Общества, виновные в нарушении режима конфиденциальности, в том числе за разглашение конфиденциальной информации, нарушение порядка обращения, утрату, незаконное уничтожение носителей конфиденциальной информации, могут быть привлечены к уголовной, административной или дисциплинарной ответственности, предусмотренной законодательством Республики Беларусь или ЛПА Общества.

Решение о применении мер дисциплинарной ответственности к виновным в нарушении режима конфиденциальности принимается Советом директоров Общества в отношении руководителей Общества или директором Общества (лицом, исполняющего его обязанности) в отношении других работников Общества в сроки согласно трудовому законодательству Республики Беларусь.

При наличии в действиях работника, виновного в нарушении режима конфиденциальности, признаков уголовного преступления директор Общества (лицо, исполняющее его обязанности) либо уполномоченные им лица имеют право обращаться в правоохранительные органы для привлечения виновного работника к ответственности в соответствии с законодательством Республики Беларусь.

58. За разглашение сведений, составляющих коммерческую тайну бывшие работники, уволенные из Общества, могут быть привлечены к ответственности в порядке, установленном законодательством Республики Беларусь.

ГЛАВА 12
ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

59. Настоящее Положение вступает в силу со дня его утверждения.

Приложение 1
к Положению о конфиденциальной
информации ЗАО «Водород»

**ПЕРЕЧЕНЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
ЗАО «ВОДОРОД»**

№ п/п	Содержание сведений	Гриф доступа	Срок действия
1.	Решения органов управления ЗАО «Водород»	КТ*	5 лет
2.	Сведения о подготовке, ведении и результатах переговоров с деловыми партнерами	КТ*	1 год
3.	Сведения, содержащиеся в учредительных документах и документах о создании ЗАО «Водород»	ДСП	постоянно
4.	Прогнозы, направления деятельности (развития) ЗАО «Водород», утвержденные органами управления ЗАО «Водород», в целом и по отдельным направлениям	КТ*	1 год
5.	Сведения из реестра владельцев ценных бумаг, иные сведения об уставном фонде, ценных бумагах ЗАО «Водород», сведения о дивидендах, начисленных на акции	ДСП	постоянно
6.	Материалы комплексных и тематических проверок (ревизий), проведенных уполномоченными органами (отчеты, докладные записки, справки и т.д.), обзорные письма о нарушениях	КТ*	5 лет
7.	Сведения об организационной и функциональной структуре, штатной численности, составе и системе оплаты труда персонала ЗАО «Водород»	КТ*	2 года
8.	Сведения о заключенных договорах, оказываемых услугах, суммах оплаты и иных условиях заключенных договоров	КТ*	1 год
9.	Сведения о финансово-хозяйственной деятельности ЗАО «Водород»	КТ*	1 год
10.	Сведения о клиентах (контрагентах) ЗАО «Водород» и их финансово-хозяйственной деятельности, информация и документы, полученные от клиентов (контрагентов) ЗАО «Водород»	КТ* / ГВС	1 год / до снятия грифа
11.	Сведения о подключениях пользователей и оборудования ЗАО «Водород» к глобальной и локальной сети передачи данных	КТ*	1 год
12.	Номера телефонов руководителей ЗАО «Водород», в том числе домашних, мобильных и IP-телефонов	КТ*	1 год
13.	Документы, регламентирующие вопросы организации защиты информации, автоматизированных, вычислительных и информационных систем, в том числе применяемых организационных методах и программно-технических средствах защиты информации и криптографические ключи	ДСП	3 года после изменения
14.	Сведения об организации, методах и средствах комплексной защиты информации от несанкционированного доступа и утечки по техническим каналам	ДСП	3 года после изменения
15.	Сведения о пропускном режиме и системе охраны, технической укрепленности, системах охранной, пожарной сигнализации, видеонаблюдения, контроля и	ДСП	3 года после изменения

№ п/п	Содержание сведений	Гриф доступа	Срок действия
	разграничения доступа в помещения, организации радиосвязи		
16.	Сведения о программном обеспечении, принципах построения, структуре и составе оборудования информационной системы ЗАО «Водород», в том числе организации администрирования и управления в вычислительных сетях	КТ*	1 год
17.	Сведения о системе организации и разграничения доступа в информационную систему ЗАО «Водород», идентификаторы и пароли, используемые сотрудниками для доступа к информации	КТ*	6 месяцев
18.	Организационно-распорядительные, справочно-информационные документы и иные материалы (инструкции, правила, методические рекомендации, презентации и т.д.), содержащие секреты производства ЗАО «Водород», ОАО «Сбер Банк», ПАО Сбербанк, переписка с ОАО «Сбер Банк» и ПАО Сбербанк»	КТ* / ГВС	1 год / до снятия грифа
19.	Информация об аффилированных лицах (инсайдерах) участников Банковского холдинга ОАО «Сбер Банк»	ГВС	до снятия грифа
20.	Материалы проверок, проведенных отделом безопасности ЗАО «Водород» и/или ОАО «Сбер Банк», в том числе по обеспечению защиты конфиденциальной информации и пропускного режима	КТ*	5 лет
21.	Сведения о методиках противодействию кибермошенничеству	КТ*	2 года
22.	Перечень правил фрод-мониторинга при совершении операций с банковскими платежными карточками, в устройствах эквайринговой сети ОАО «Сбер Банк», в системах дистанционного банковского обслуживания физических и юридических лиц	ГВС	до снятия грифа
23.	Сведения об инцидентах в области кибермошенничества	КТ*	6 месяцев
24.	Заявления о потенциальных конфликтах интересов работников ЗАО «Водород»	КТ*	3 года
25.	Сведения, составляющие в соответствии со статьей 121 Банковского кодекса Республики Беларусь банковскую тайну, в том числе по операциям с использованием банковских платежных карточек	ДСП**	постоянно
26.	Сведения о частной жизни физических лиц и персональные данные	ДСП**	постоянно

Расшифровка грифов ограничения доступа:
ДСП – для служебного пользования
КТ – коммерческая тайна
ГВС – гриф владельца сведений

Примечания:
<*> Необходимость отнесения сведений к конфиденциальной информации и присвоения документам грифа ограничения доступа определяется исполнителем.
<**> Гриф ограничения доступа ДСП устанавливается на исходящих документах, направляемых в сторонние организации (ответах на запросы уполномоченных государственных органов и т.д.).

Приложение 2
к Положению о конфиденциальной
информации ЗАО «Водород»

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации

Я, _____
(фамилия, имя, отчество (если таковое имеется), дата рождения,

_____
идентификационный номер (для граждан Республики Беларусь), серия и номер паспорта,

_____ ,
адрес места регистрации и места жительства, если последнее отличается от места регистрации)

вступая в трудовые отношения с ЗАО «Водород» (далее – Общество), **обязуюсь**:

1. Выполнять требования законодательства Республики Беларусь и иных нормативных правовых актов Республики Беларусь, локальных правовых актов Общества, регламентирующих вопросы ограничения доступа к сведениям, составляющим банковскую тайну, конфиденциальную информацию о депонентах и другие профессиональные тайны, коммерческую тайну Общества, служебную информацию ограниченного распространения, информацию о частной жизни физических лиц и персональные данные, иных сведений, распространение которых ограничено в соответствии с законодательством Республики Беларусь, а также конфиденциальную информацию третьих лиц, к которым Общество получило доступ (далее – конфиденциальная информация).

2. Выполнять требования установленного в Обществе режима конфиденциальности, не разглашать конфиденциальную информацию, к которой получил доступ в процессе служебной деятельности в Обществе, в том числе в ходе аудиторских, ревизионных и иных проверок, третьим лицам, в том числе другим работникам Общества, не имеющим к ней отношения.

3. Без соответствующего разрешения не раскрывать и не передавать работникам других организаций и иным лицам, не размещать и не обсуждать в средствах массовой информации (печатные издания, радио и телевидение), в других открытых источниках информации, в том числе в сети Интернет, социальных сетях, форумах и т.п., служебные вопросы и иные сведения о деятельности Общества, независимо от ее конфиденциальности, а также не использовать технические средства (мобильные телефоны, фотоаппараты, планшеты, диктофоны и т.п.) для осуществления аудио-, фото- и видеофиксации в служебных помещениях Общества.

4. Не использовать сведения, ставшие известными в процессе служебной деятельности в Обществе, в целях, не связанных с выполнением должностных обязанностей.

5. Не предоставлять выданные мне программно-технические средства и сведения (идентификаторы и пароли доступа, личный ключ электронной цифровой подписи и т.д.), необходимые для доступа к информационным ресурсам Общества и использования электронной цифровой подписи, третьим лицам, включая других работников Общества, членов семьи, знакомых и т.д.

6. Не передавать конфиденциальную информацию по незащищенным каналам связи и передачи информации (радиосвязь, телефонные и факсимильные линии связи, электронная почта и т.п.).

7. Не выносить без соответствующего разрешения за пределы помещений Общества носители конфиденциальной информации.

8. Вернуть по требованию Общества или при прекращении трудового договора (контракта) все находящиеся у меня носители конфиденциальной информации, в том числе копии, выписки, черновики и т.д.

9. Сообщать немедленно, а при невозможности – в кратчайшие сроки непосредственному руководителю и в отдел безопасности Общества о (об):

9.1. допущенных мною или ставших мне известными нарушениях режима конфиденциальности, в том числе установленных правил обращения с носителями конфиденциальной информации, разглашения (угрозы разглашения) конфиденциальной информации, незаконного ознакомления с конфиденциальной информацией, или незаконного использования конфиденциальной информации;

9.2. требованиях иных лиц предоставить им незаконный доступ к конфиденциальной информации, в том числе попытках этих лиц получить такой доступ под угрозой применения насилия или совершения иного противоправного действия, посредством обещания незаконного вознаграждения (материального либо путем предоставления услуги) и т.п.;

9.3. об утрате:

носителей конфиденциальной информации, в том числе отдельных листов документов, содержащих конфиденциальную информацию;

служебного удостоверения или постоянного (временного) пропуска;

личной печати;

ключей от служебных помещений, сейфовых комнат, сейфов (шкафов) и иных хранилищ, в которых хранятся носители конфиденциальной информации, в том числе электронных ключей доступа и электронных ключей управления роллетами;

программно-технических средств и сведений, необходимых для доступа к информационным ресурсам Общества, в том числе электронной цифровой подписи.

Я предупрежден(а) о возможности в целях контроля соблюдения мною требований режима конфиденциальности применения в отношении меня аудио- и видеоконтроля, технологического контроля информации,

циркулирующей в корпоративных сетях связи и передачи информации (корпоративной телефонной и локальной вычислительной сетях, персональном компьютере и т.п.), иных не запрещенных законодательством технических средств и методов защиты информации, а также других мер, не противоречащих законодательству, **и согласен(а)** на данную форму контроля со стороны Общества.

Я ознакомлен(а) с Перечнем конфиденциальной информации ЗАО «Водород».

Я подтверждаю, что со мной проведен инструктаж, в рамках которого **я ознакомлен(а)** с нормами законодательных актов Республики Беларусь, Положения о конфиденциальной информации ЗАО «Водород» и других локальных правовых актов Общества, регламентирующих вопросы режима конфиденциальности, в том числе в части возложения на меня как работника Общества соответствующих обязанностей, а также ответственности за нарушение установленного режима конфиденциальности и/или разглашение (утрату) конфиденциальной информации.

«____» _____ 20___ _____ _____

подпись *ФИО*

Приложение 3
к Положению о конфиденциальной
информации ЗАО «Водород»

ТИПОВАЯ ФОРМА СОГЛАШЕНИЯ О КОНФИДЕНЦИАЛЬНОСТИ

Закрытое акционерное общество «Водород», именуемое в дальнейшем Заказчик, в лице директора _____, действующего на основании Устава, с одной стороны, и _____ _____, именуемое в дальнейшем Исполнитель, в лице_____, действующего на основании _____, с другой стороны, вместе именуемые по тексту Стороны, заключили настоящее Соглашение конфиденциальности и неразглашении информации (далее – Соглашение).

Статья 1. Определения и термины

1.1. **Документ** – бумажный, электронный или любой иной носитель информации, позволяющий ее индивидуализировать.

1.2. **Конфиденциальная информация** – любая документированная, то есть зафиксированная в документе информация, и обозначенная Раскрывающей стороной как «Конфиденциальная» (включая, но не ограничиваясь, информацию, относящуюся к бизнес- либо финансовым планам и стратегиям, включая, без ограничений, информацию о рынках, финансовых документах, финансовой отчетности и учету (за исключением случаев установленных законодательством); ценообразованию и маркетингу товаров (работ, услуг), техническую информацию, коммерческие секреты, ноу-хау, исследования, производственные планы, концепты, объекты интеллектуальной деятельности (в том числе открытия, изобретения, рационализаторские предложения, полезные модели, конструкции, промышленные образцы, не запатентованные по каким-либо мотивам, программное обеспечение (компьютерные программы), базы данных, эскизы товарных знаков, не зарегистрированные по каким-либо причинам), а также информация о договорах, заключенных между Сторонами; информация о ходе их выполнения и полученных результатах, стоимости работ / услуг, технических условиях; персональные данные), передаваемая Раскрывающей стороной Получающей стороне, в отношении которой соблюдаются следующие условия:

данная информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;

данная информация не относится к категории общедоступной;

данная информация может быть в соответствии с законодательством Республики Беларусь отнесена к конфиденциальной информации;

данная информация не находилась в распоряжении Получающей стороны до ее предоставления Раскрывающей стороной в рамках Соглашения.

К конфиденциальной информации не относится информация, которая стала общеизвестной, доступ к которой был предоставлен Раскрывающей стороной третьим лицам без ограничений либо иным способом ставшая общедоступной не по вине Получающей стороны (но не ранее ее публичного распространения).

Не относится к конфиденциальной также информация, в отношении которой Получающей стороной может быть доказано, что она была создана Получающей стороной без обращения к конфиденциальной информации.

1.3. **Обязательство о неразглашении конфиденциальной информации** – документ, подписываемый Стороной с Представителем и закрепляющий обязательство Представителя о неразглашении конфиденциальной информации, а также ответственность за ее разглашение. Обязательство о неразглашении конфиденциальной информации с Представителем, который является физическим лицом, заключается по форме установленной Стороной самостоятельно.

1.4. **Получающая сторона** – сторона, получающая конфиденциальную информацию.

1.5. **Представитель / Филиал** – любой работник, уполномоченный представитель или самостоятельное структурное подразделение Стороны, а равно подрядчик либо иное лицо, работающее по гражданско-правовому договору, включая любое физическое или юридическое лицо, который прямо или косвенно контролирует деятельность или находится под контролем Исполнителя.

1.6. **Разглашение конфиденциальной информации** – любое действие или бездействие Получающей стороны, в результате которого конфиденциальная информация в любой возможной форме (устной, письменной, электронной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам, без согласия Раскрывающей стороны.

1.7. **Разрешенное использование** – предпринимаемые Стороной действия исключительно в целях своей внутренней, хозяйственной деятельности, либо по поручению другой Стороны, а также по требованию государственных органов Республики Беларусь на основании соответствующего законодательства.

1.8. **Раскрывающая сторона** – сторона, которая передает конфиденциальную информацию.

Статья 2. Предмет Соглашения

2.1. На условиях Соглашения Заказчик предоставляет Исполнителю доступ к конфиденциальной информации, в том числе размещенной в информационной системе Заказчика и/или клиентов Заказчика и конфиденциальной документации, а также к ресурсам ИС.

Доступ к конфиденциальной информации, размещенной в информационной системе клиента Заказчика, предоставляется только с письменного разрешения данного клиента.

2.2. Стороны предоставляют друг другу доступ к конфиденциальной информации и конфиденциальной документации исключительно в режиме разрешенного использования в соответствии с условиями Соглашения.

2.3. Вся конфиденциальная информация, предоставляемая Получающей стороне в какой-либо форме согласно Соглашению, является и остается собственностью Раскрывающей стороны. Другая Сторона не обладает никакими правами собственности или другими правами на конфиденциальную информацию и конфиденциальную документацию, а также обязуется пользоваться полученными сведениями, не нарушая интересов Стороны, предоставившей информацию.

2.4. На период действия Соглашения, а также в течение 5 (пяти) лет после истечения срока его действия Стороны обязуются не разглашать каким-либо третьим лицам, кроме своих работников, учредителей, конфиденциальную информацию. Стороны предпримут все необходимые меры для целей обеспечения, как со своей стороны, так и со стороны своих филиалов, не предоставления и/или не раскрытия любому лицу в любой форме, прямо или косвенно любого аспекта конфиденциальной информации и конфиденциальной документации. Положения настоящего пункта остаются в силе и после прекращения действия Соглашения и независимо от оснований такого прекращения.

Статья 3. Порядок передачи и использования конфиденциальной информации

3.1. Раскрывающая сторона передает Получающей стороне конфиденциальную информацию на бумажных, электронных, магнитных и других носителях. Передача конфиденциальной информации или конфиденциальной документации может оформляться актом приема-передачи.

3.2. Получающая сторона может предоставлять доступ к конфиденциальной информации только своим Представителям, которым необходимо иметь доступ к конфиденциальной информации при выполнении своих должностных обязанностей для достижения цели предоставления конфиденциальной информации, подписавшим Обязательство о неразглашении конфиденциальной информации и уведомленным о факте заключения Соглашения. По требованию Раскрывающей стороны Получающая сторона обязана предоставить список вышеуказанных Представителей.

3.3. С момента подписания Соглашения любая информация, обозначенная как «Конфиденциальная» и не являвшаяся до этого достоянием общественности / общеизвестной, полученная Получающей стороной от Раскрывающей стороны, является конфиденциальной и без соответствующего предварительного письменного согласия Раскрывающей стороны не подлежит разглашению третьим лицам (физическим и/или юридическим лицам), за исключением случаев ее предоставления в соответствии с требованиями законодательства Республики Беларусь уполномоченным на истребование

такой информации государственным органам Республики Беларусь, а также Представителям Сторон, с которыми заключено обязательство о неразглашении конфиденциальной информации. При наличии у Получающей стороны сомнений относительно того, является ли информация конфиденциальной, Получающая сторона обязана запросить соответствующие разъяснения у Раскрывающей стороны.

3.4. Стороны обязуются предпринимать все соответствующие меры предосторожности с целью предотвращения несанкционированного раскрытия или разглашения конфиденциальной информации любому из своих филиалов и/или третьим лицам.

3.5. Полные или частичные копии любых конфиденциальных документов подлежат учету и защите так же, как и их оригиналы.

3.6. Раскрытие конфиденциальной информации или конфиденциальной документации третьей стороне разрешается только с письменного согласия Стороны, предоставившей информацию.

3.7. Раскрывающая сторона имеет право требовать в любое время возврата конфиденциальной информации путем направления письменного уведомления в адрес Получающей стороны. При этом Получающая сторона обязана в течение 10 (десяти) рабочих дней с даты получения такого уведомления возвратить Раскрывающей стороне конфиденциальную информацию в полном объеме, а также все копии и репродукции с документов, содержащих конфиденциальную информацию, находящихся у Получающей стороны.

3.8. Исполнитель обязан в любое время по запросу Заказчика предоставить последнему доступ ко всем своим сведениям, созданным при помощи прямого или косвенного использования конфиденциальной информации и конфиденциальной документации Заказчика.

3.9. Любая информация и документация, в том числе их копии, составляющая конфиденциальную информацию и не используемые Исполнителем, должны быть возвращены Заказчику.

3.10. По истечении срока действия Соглашения, а также в случае его досрочного расторжения Стороны обязаны в течение 1 (одного) рабочего дня вернуть друг другу по акту приема-передачи, который является неотъемлемой частью Соглашения, все оригиналы и копии конфиденциальной документации, в чьем бы распоряжении они ни находились, а также всю конфиденциальную информацию, если они передавались ранее по акту-приема передачи.

3.11. В целях поддержания должного уровня информационной безопасности Заказчика Исполнитель обязуется при использовании конфиденциальной информации соблюдать следующие правила безопасности:

3.11.1. организовать защиту периметра своей вычислительной сети, обеспечивающую защищенность внутренних информационных ресурсов Исполнителя и Заказчика;

3.11.2. обеспечивать тайну конфиденциальной информации, путем ограниченного доступа к ней должностных лиц и работников/представителей Исполнителя, и соответствующего хранения конфиденциальной информации на бумажных и электронных носителях;

3.11.3. заключить со своими работниками и/или Представителями обязательство о неразглашении конфиденциальной информации по форме в соответствии с законодательством, регулирующем отношения Исполнителя с соответствующим физическим лицом и/или Представителем;

3.11.4. предоставить Заказчику по его требованию копии документов, подтверждающих выполнение обязанностей, предусмотренных подпунктом 11.3. настоящего пункта;

3.11.5. направить Заказчику по его письменному запросу список работников и/или Представителей, привлеченных Исполнителем к выполнению работ/оказанию услуг;

3.11.6. не копировать и не разглашать кому-либо содержание документов Заказчика, не относящихся к деятельности Исполнителя;

3.11.7. соблюдать такую же высокую степень тайны во избежание разглашения или использования конфиденциальной информации, какую Получающая сторона соблюдала бы в разумной степени в отношении своей собственной конфиденциальной информации такой же степени важности;

3.11.8. уведомить в незамедлительном порядке Раскрывающую сторону о требованиях третьих лиц, предъявленных Получающей стороне в связи с раскрытием конфиденциальной информации Раскрывающей стороной;

3.11.9. прекратить по письменному требованию раскрывающей Стороны использование конфиденциальной информации, вернуть конфиденциальную информацию и все копии, записи и выдержки из нее Раскрывающей стороне, и по требованию Раскрывающей стороны, подтвердить в письменной форме тот факт, что Получающая сторона выполнила все обязательства, изложенные в настоящем пункте.

Статья 4. Изъятие из режима конфиденциальности

4.1. Условия Соглашения не распространяются на любые сведения, информацию, процессы, ноу-хау, составляющие часть конфиденциальной информации, которые на дату подписания Соглашения или позднее стали широко известны с согласия Стороны, предоставившей сведения, в связи с которыми Сторона предоставит документальное или другое бесспорное подтверждение того факта, что Исполнитель на законных основаниях и без каких-либо обязательств по отношению к другой Стороне владеет такой информацией.

4.2. Если Сторона объявляет о том, что она не связана обязательствами по Соглашению в отношении конфиденциальной информации в связи с условиями предусмотренными пунктом 4.1 настоящей статьи, то она обязана направить письменное уведомление об этом другой Стороне вместе с документальными подтверждениями не позднее, чем через 10 (десять) дней с даты получения конфиденциальной информации.

4.3. Просрочка или отсутствие уведомления, предусмотренного пунктом 4.2 настоящей статьи, независимо от сроков просрочки, рассматривается в качестве признания Исполнителем своих обязательств по Соглашению в отношении сведений/информации, предусмотренных в пункте 4.1 настоящей статьи.

Статья 5. Ответственность сторон

5.1. В случае утечки конфиденциальной информации по вине Получающей стороны независимо от того, вызвано это умышленными, неосторожными или самонадеянными действиями и наличия у Раскрывающей стороны доказательств совершения Получающей стороной виновных действий, виновная сторона обязана возместить пострадавшей стороне документально подтвержденные убытки.

5.2. Стороны несут ответственность за разглашение и сохранность конфиденциальной информации как в период действия Соглашения, так и в течение 5 (пяти) лет по окончании его действия.

5.3. В случаях выявления Заказчиком фактов нарушения Исполнителем условий Соглашения Заказчик вправе:

5.3.1. истребовать от Исполнителя в соответствии с законодательством Республики Беларусь полного возмещения причиненного Заказчику документально подтвержденного ущерба, если таковой нанесен из-за несоблюдения Исполнителем норм информационной безопасности, оговоренных Соглашением и уплаты штрафа в размере десяти тысяч базовых величин на день оплаты за каждый случай нарушения;

5.3.2. в одностороннем порядке отказаться от исполнения любых договоров (соглашений), заключенных между Сторонами, в рамках которых Исполнитель должен получить или получил доступ к конфиденциальной информации.

5.4. Любое одностороннее расторжение или отказ какой-либо из сторон от исполнения обязательств по сделкам, заключенным Сторонами после заключения Соглашения, в связи с нарушением или ненадлежащим исполнением обязательств другой стороной по Соглашению при условии включения таких условий в вышеуказанные сделки, не будут рассматриваться в качестве неисполнения обязательств.

Статья 6. Порядок разрешения споров

6.1. Все споры и разногласия по Соглашению Стороны решают путем переговоров.

6.2. В случае невозможности разрешения разногласий путем переговоров, они подлежат рассмотрению в Экономическом суде города Минска (Республика Беларусь).

Статья 7. Обстоятельства непреодолимой силы

7.1. Стороны освобождаются от ответственности по Соглашению в случае возникновения чрезвычайных и непредотвратимых при данных условиях обстоятельств (форс-мажор). Сторона, для которой создалась невозможность исполнения обязательств по Соглашению, обязана не позднее десяти (10) дней с момента их наступления в письменной форме уведомить об этом другую Сторону. Не уведомление или несвоевременное уведомление о невозможности исполнения обязательств по Соглашению в связи с форс-мажором лишает Сторону права ссылаться на такое обстоятельство как на основание, освобождающее ее от ответственности за неисполнение обязательств по Соглашению.

Статья 8. Срок действия соглашения

8.1. Соглашение считается заключенным и вступает в силу с момента его подписания. Момент подписания определяется датой, указанной на первой странице текста Соглашения.

8.2. Соглашение действует в течение срока действия договоров, заключенных между Сторонами, а в случае отсутствия таких договоров – в течение 5 (пяти) лет с даты его подписания.

8.3. В случае наличия предусмотренных Соглашением оснований для одностороннего отказа от Соглашения, Сторона-инициатор одностороннего отказа от Соглашения обязана уведомить другую Сторону о своем намерении не позднее, чем за 15 (пятнадцать) календарных дней до предполагаемой даты расторжения Соглашения. При этом неисполненные по Соглашению обязательства должны быть завершены, если иное не предусмотрено дополнительным соглашением Сторон.

Статья 9. Дополнительные условия

9.1. Односторонний отказ от обязательств не допускается, за исключением случаев, предусмотренных Соглашением.

9.2. Все изменения и дополнения к Соглашению действительны только в том случае, если они совершены в письменной форме и подписаны Сторонами или их полномочными представителями. Надлежащим образом оформленные изменения и дополнения к Соглашению являются его неотъемлемой частью.

9.3. В случае противоречия условий о конфиденциальности, содержащихся в договорах (соглашениях), заключенных между Сторонами, в рамках которых Получающая сторона должна получить или получила доступ к конфиденциальной информации, и в Соглашении, действуют условия Соглашения.

9.4. После подписания Соглашения обеими Сторонами все предшествующие переговоры и переписка по вопросам, урегулированным Соглашением, утрачивают юридическую силу.

9.5. Условия Соглашения распространяются на все правоотношения между Сторонами и все заключенные Сторонами договоры (соглашения), в рамках которых передается конфиденциальная информация.

9.6. Заголовки статей Соглашения предназначены для удобства пользования текстом и не будут приниматься во внимание при толковании положений Соглашения.

9.7. Передача одной из Сторон прав по Соглашению третьим юридическим и/или физическим лицам не допускается, за исключением случаев, когда на это имеется письменное согласие другой Стороны.

9.8. Все уведомления Сторонами друг друга по Соглашению должны совершаться в письменной форме, подписываться надлежащими представителями Сторон и направляться по указанным в Соглашении юридическим адресам Сторон.

Стороны обязаны незамедлительно информировать друг друга в письменной форме о любых изменениях юридического адреса, юридического статуса или банковских реквизитов, подчиненности, а также предоставлять уполномочивающие документы (доверенности) для своих представителей на переговорах для подписания финансовых и обязательственных документов.

9.9. Стороны до получения оригиналов соответствующих документов признают обязательную юридическую силу документов (в том числе уведомлений), направленных по электронной почте, факсу или иным электронным каналам связи при условии, что такие документы скреплены/заверены подписью уполномоченных представителей Сторон и оттиском печати соответствующей Стороны, а также содержат иные реквизиты, которые позволяют достоверно установить, что документы исходят от соответствующей Стороны.

9.10. Положения Соглашения являются конфиденциальными. Каждая из Сторон примет все необходимые меры для того, чтобы предотвратить ознакомление с Соглашением (в том числе дополнениями и приложениями к нему), третьих лиц без согласия на этом другой Стороны, за исключением случаев, предусмотренных законодательством Республики Беларусь.

9.11. Правом, применимым к правоотношениям Сторон, вытекающим из или в связи с действием Соглашения, является право Республики Беларусь.

9.12. Соглашение составлено на русском языке в двух экземплярах, имеющих одинаковую юридическую силу, по одному для Исполнителя и Заказчика.

Статья 10. Юридические адреса, реквизиты и подписи сторон

Сторона – 1	Сторона – 2
(реквизиты Стороны)	*(реквизиты Стороны)*
_____ _____	_____ _____
(подпись) *(И.О.Фамилия)*	*(подпись)* *(И.О.Фамилия)*
(печать)	(печать)

Приложение 4
к Положению о конфиденциальной
информации ЗАО «Водород»

ТИПОВАЯ ФОРМА РАЗДЕЛА О КОНФИДЕНЦИАЛЬНОСТИ

1. Конфиденциальная информация – любые материалы, а также коммерческая, финансовая, техническая, технологическая, экономическая, организационная и другая охраняемая законом информация, включая служебную информацию ограниченного распространения, коммерческую тайну, профессиональные тайны, снабженная грифом ограничения доступа («Коммерческая тайна», «Конфиденциально», «Для служебного пользования» и др.) (далее – гриф ограничения доступа) или иным образом обозначенная как конфиденциальная информация, а также иная информация подлежащая защите в соответствии с требованиями законодательства, касающаяся Стороны, передающей информацию (далее – Передающая Сторона), ее деятельности, переданная другой Стороне договора (далее – Получающая Сторона) в устной, письменной, визуальной или другой форме, записанная в любой форме и на любом носителе информации (в том числе в форме презентаций, схем, фильмов, документов или в электронной форме) непосредственно Стороной или посредственно лицом, действующим от ее имени, либо другим образом полученная от Передающей Стороны, а также информация, подготовленная на основании предоставленной Передающей Стороной информации и содержащая или отражающая информацию, предоставленную Передающей Стороной.

Информация не является конфиденциальной в случае, если информация:

- является или стала общеизвестной до подписания настоящего контракта (договора), а также не в результате его нарушения (но не ранее ее публичного распространения);
- находилась в распоряжении Получающей Стороны до ее получения от Передающей Стороны и была получена законным способом без нарушения каких-либо обязательств по сохранению конфиденциальности;
- получена Получающей Стороной из независимых источников или от третьих лиц без обязательств по сохранению конфиденциальности, а также в отношении которых у Получающей Стороны не было сведений о неправомерном раскрытии такими источниками или лицами данной информации;
- в отношении которой Получающей стороной может быть доказано, что она была создана Получающей стороной без доступа к Конфиденциальной информации Передающей Стороны и без ее использования;
- в отношении которой Получающей стороной получено письменное разрешение (в том числе согласован объем и содержание материалов) Передающей стороны на ее разглашение (распространение, опубликование и т.д.).

2. Получающая Сторона обязуется:

сохранять в тайне, не раскрывать и не разглашать Конфиденциальную информацию и ее источники, принять для обеспечения сохранности Конфиденциальной информации меры, не меньшие, чем те, которые Получающая сторона принимает для обеспечения сохранности своей собственной Конфиденциальной информации;

обеспечить достоверный учет Конфиденциальной информации, копий, выписок или иных материалов (в том числе в электронном виде), содержащих Конфиденциальную информацию, надежное хранение, ограничение доступа работников, не имеющих к ней отношения, а также любых третьих лиц, в том числе в нерабочее время;

использовать Конфиденциальную информацию исключительно для достижения цели настоящего договора;

по письменному требованию Передающей стороны немедленно вернуть или уничтожить документы, содержащие любые их копии, выписки или иные материалы;

незамедлительно сообщить о допущенных либо ставших известными фактах незаконного ознакомления с Конфиденциальной информацией, фактах незаконного использования Конфиденциальной информации, фактах разглашения или угрозы разглашения конфиденциальной информации третьим лицам и предпринятых мерах по уменьшению ущерба.

3. При необходимости привлечения третьих лиц (субподрядчиков, соисполнителей и т.д.) для достижения цели настоящего договора с обеспечением их доступа к Конфиденциальной информации, заблаговременно проинформировать Передающую сторону. Доступ третьих лиц к Конфиденциальной информации предоставляется только после письменного разрешения Передающей Стороны.

4. По запросу Передающей Стороны, для обеспечения доступа к конфиденциальной информации работников Получающей Стороны и третьих лиц (субподрядчиков, соисполнителей и т.д.), предоставить паспортные и другие данные, а также предусмотренные нормативными правовыми актами Республики Беларусь письменные согласия на предоставление сведений из информационных ресурсов, находящихся в ведении Министерства внутренних дел Республики Беларусь и Национального банка Республики Беларусь.

5. Стороны несут полную ответственность за действия (бездействие) своих работников и третьих лиц, привлекаемых ими для выполнения договорных обязательств.

6. Сторона, не исполнившая свои обязательства по обеспечению Конфиденциальности, обязана возместить другой Стороне убытки, причиненные разглашением или неправомерным использованием Конфиденциальной информации. Убытки возмещаются в соответствии с законодательством Республики Беларусь.

7. Завершение договорных отношений не влечет изменения (прекращения) обязанностей Сторон по соблюдению требований Конфиденциальности, установленных настоящим контрактом (договором).

Приложение 5
к Положению о конфиденциальной
информации ЗАО «Водород»

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ИНФОРМАЦИОНЫМИ РЕСУРСАМИ ЗАО «ВОДОРОД», СОДЕРЖАЩИМИ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Правила информационной безопасности разработаны в соответствии с законодательством Республики Беларусь, регулирующим деятельность в области защиты информации и информатизации.

Настоящие Правила определяют основные принципы обеспечения информационной безопасности в том числе:

правила доступа к ресурсам информационной системы ЗАО «Водород» (далее – Общество);

общие обязанности пользователей при работе с ресурсами информационной системы Общества;

требования к идентификаторам и паролям доступа пользователей информационной системы Общества;

порядок использования системы электронной почты и ресурсов глобальной сети Интернет;

обязательство информирования об инцидентах в области информационной безопасности;

ответственность за нарушение правил информационной безопасности.

ГЛАВА 2
ПРАВИЛА ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К РЕСУРСАМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЩЕСТВА

2. Подключение компьютерной техники к корпоративной сети Общества согласуется с отделом безопасности Общества.

3. Доступ пользователей к ресурсам информационной системы (далее – ИС) Общества осуществляется в соответствии с установленным порядком.

4. Доступ к конфиденциальной информации может быть предоставлен пользователям, принявшим обязательство о неразглашении конфиденциальной информации, при условии соблюдения требований законодательства Республики Беларусь, регулирующих вопросы ограничения распространения определенных категорий сведений (служебной информации ограниченного распространения, профессиональной тайны, коммерческой тайны, информация о частной жизни физического лица и персональных данных и т.д.).

5. На компьютерах пользователей устанавливается специализированное программное обеспечение, ограничивающее доступ пользователей к внешним носителям информации.

В случае служебной необходимости предоставление пользователю внешнего носителя информации и прав доступа к нему осуществляется в соответствии с установленным в Обществе порядком.

6. С целью исключения несанкционированного вскрытия, корпус компьютера опечатывается пломбой либо самоклеющимся стикером (одноразовым опечатывающим материалом).

7. Настоящие Правила обязательны для исполнения всеми пользователями ИС Общества.

ГЛАВА 3
ОБЩИЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ПРИ РАБОТЕ С РЕСУРСАМИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЩЕСТВА

8. Все компоненты ИС Общества должны использоваться пользователями только для достижения целей гражданско-правового договора, в рамках которого необходим доступ к ресурсам ИС Общества.

9. При работе в ИС Общества пользователь обязан руководствоваться следующими принципами:

9.1. знать и исполнять требования настоящих Правил, а также инструкции и руководства по эксплуатации персональных компьютеров, принтеров, сканеров, модемов и другой техники (далее – технические средства);

9.2. обеспечивать неизменность программной конфигурации (сохранение текущих установок) выданных ему технических средств;

9.3. соблюдать требования, предъявляемые к идентификаторам и паролям доступа, изложенные в главе 4 настоящих Правил;

10. При работе в ИС Общества пользователю запрещается:

10.1. самостоятельно устанавливать программное обеспечение (далее – ПО);

10.2. самостоятельно удалять либо изменять конфигурацию ПО;

10.3. нарушать правила корректного завершения работы или принудительно прерывать выполнение ПО;

10.4. самостоятельно разбирать, разукомплектовывать, перемещать технические средства или производить установку дополнительного оборудования, а также отключать или подсоединять разъемы;

10.5. использовать технические средства и информационные ресурсы в неслужебных целях (для компьютерных игр; получения, отправки информации, не связанной с исполнением обязательств по договору и т.д.);

10.6. допускать к работе на компьютере посторонних лиц (в том числе других пользователей, за исключением случаев, связанных с выполнением последними своих должностных обязанностей);

10.7. передавать (сообщать) кому-либо персональные идентификаторы доступа (электронные ключи, уникальное имя (идентификатор), пароль и т.п.);

10.8. выносить (копировать на сменные носители, пересылать посредством электронной почты либо иным способом) за пределы Общества служебную информацию, включая конфиденциальную информацию, без соответствующего разрешения;

10.9. приносить, использовать и/или распространять в Обществе информацию в электронном виде (файлы), не связанную с исполнением обязательств по договору.

ГЛАВА 4
ТРЕБОВАНИЯ К ИДЕНТИФИКАТОРАМ И ПАРОЛЯМ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБЩЕСТВА

11. Каждому пользователю ИС Общества назначается уникальное имя (идентификатор).

Первоначальное присвоение пароля пользователю осуществляет администратор. При первой регистрации, которая должна быть произведена в течение одного рабочего дня с момента подключения пользователя к информационному ресурсу, он обязан сменить пароль с учетом требований п. 12 настоящих Правил.

12. Запрещается использовать в качестве пароля:

12.1. нулевой пароль (не имеющий значения);

12.2. пароль, содержащий менее 12 символов

12.3. идентификатор доступа;

12.4. собственное имя, фамилию (родственников или близких), дату рождения;

12.5. номер паспорта, телефона, автомобиля и т.д.;

12.6. названия улиц, городов, стран, а также месяцев, дней недели, знаков зодиака (гороскопов) и т.д.;

12.7. названия известных продуктов и фирм (автомобили, косметические изделия и т.д.);

12.8. имена персонажей популярных книг, кинофильмов, названия спортивных команд и т.д.;

12.9. слова, связанные с обеспечением безопасности («Секрет», «Пароль», «password» и т.д.), а также непосредственно с работой («Банк», «Кредит» и т.д.);

12.10. применять зеркальное отображение вышеуказанных слов (названий);

12.11. использовать повторение 3 (трех) и более одинаковых символов.

13. Пользователь обязан:

13.1. самостоятельно менять все используемые пароли не реже одного раза в три месяца (90 дней);

13.2. держать пароль в тайне.

14. Пользователю запрещается:

14.1. записывать пароли;

14.2. вводить пароль при посторонних, в случае невозможности обеспечить скрытность при вводе.

15. При утрате (забыл, пароль заблокирован и т.п.) пользователем пароля доступа к ресурсам ИС Общества сброс (разблокировка) пароля осуществляется по запросу, подготовленному ответственным работником подразделения Общества, инициировавшего заключение договора, на основании которого получен доступ к информационным ресурсам Общества.

ГЛАВА 5
ПОРЯДОК ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ЭЛЕКТРОННОЙ ПОЧТЫ И РЕСУРСОВ ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

16. Доступ пользователей к информационным ресурсам глобальной сети Интернет в ИС Общества ограничивается посредством специализированного ПО.

17. При использовании систем электронной почты и работе в глобальной сети Интернет в рамках ИС Общества пользователями должны быть выполнены следующие требования:

17.1. в качестве почтовых серверов и почтовых клиентов использовать программный комплекс Lotus Notes;

17.2. проявлять осторожность при работе с входящей корреспонденцией, рекомендуется не открывать (игнорировать) либо удалять незапрашиваемые почтовые сообщения от неизвестных адресатов;

17.3. для доступа к ресурсам глобальной сети Интернет использовать только протоколы http (протокол работы с WWW серверами) и ftp (протокол обмена файлами);

17.4. доступ к информационным ресурсам глобальной сети Интернет осуществлять только с использованием оборудования, установленного в центральном аппарате Общества.

18. Пользователям запрещено:

18.1. использовать ресурсы глобальной сети Интернет, посылать либо получать информацию, в том числе с использованием системы электронной почты, в целях не связанных с выполнением обязательств по договору:

18.2. сообщать свой почтовый адрес либо почтовые адреса других пользователей в ситуациях, не связанных с выполнением обязательств по договору;

18.3. использовать клиентов Peer-to-Peer сетей (файлообменные сети) и ПО, использующее протоколы Instant Messaging (ПО мгновенного обмена текстовыми сообщениями).

ГЛАВА 6
ИНФОРМИРОВАНИЕ ОБ ИНЦИДЕНТАХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

19. При возникновении подозрения, что инцидент, угрожающий информационной безопасности Общества, происходит, произошел или

возможен, пользователь обязан связаться с работником отдела безопасности Общества для локализации потенциально вредного воздействия на ИС Общества.

20. Пользователи не должны пытаться самостоятельно расследовать инциденты в области информационной безопасности или принимать какие-либо ответные действия.

ГЛАВА 7
ОТВЕТСТВЕННОСТЬ

21. При нарушении настоящих Правил пользователем ему блокируется доступ к ресурсам ИС Общества. Об инциденте уведомляется руководство организации-нанимателя.

22. Пользователь ИС Общества несет персональную ответственность за сохранность выданных ему для работы технических средств.

23. Пользователи, использующие глобальные и корпоративные сети в целях, не связанных с исполнением должностных обязанностей, лишаются прав доступа к указанным информационным ресурсам.

Ответственность за несанкционированный доступ к любым информационным ресурсам несут пользователь, осуществивший доступ, а также пользователь, с чьим идентификатором и паролем доступ был осуществлен.

8. МЕСТО НАХОЖДЕНИЯ, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Сторона – 1	Сторона – 2
(реквизиты Стороны)	*(реквизиты Стороны)*
_____ _____	_____ _____
(подпись) *(И.О.Фамилия)*	*(подпись)* *(И.О.Фамилия)*
(печать)	(печать)

Приложение 6
к Положению о конфиденциальной
информации ЗАО «Водород»

АКТ
приема-передачи конфиденциальной информации

г. Минск _____ 20__ г.

_____, именуемое в дальнейшем Сторона-1, в лице _____, действующего на основании _____, с одной стороны, и Закрытое акционерное общество «Водород», именуемое в дальнейшем Сторона-2, в лице_____, действующего на основании_____, с другой стороны, далее совместно именуемые Стороны, а в отдельности – Сторона, составили настоящий акт к Соглашению о конфиденциальности от «___»_____ 20___ г. (далее – Соглашение) о нижеследующем:

1. Сторона-1 передала, а Сторона-2 приняла следующую документацию (информацию):

_____

(листов в документе, регистрационный номер, иные сведения)

2. Сведения о передаче:

1	Категории конфиденциальной информации	
2	Цели передачи (передач)	1. 2. (в случае осуществления передачи персональных данных перечисляются все цели для которых они передаются)
3	Состав персональных данных (при наличии)	1. Фамилия, имя, отчество (ФИО). 2. Серия, номер документа, удостоверяющего личность. 3. Место жительства. 4. Номер мобильного телефона и иные сведения (отнесенные в соответствии с законодательством к персональным данным)
4	Наличие согласия субъекта персональных данных на обработку персональных данных у передающей стороны	

5	Наличие согласия владельца на передачу сведений составляющих банковскую тайну	
6	Способ передачи	
7	Срок обработки персональных данных	
8	Правовые основания для передачи персональных данных	
9	Периодичность передачи информации	
10	Иные условия обработки персональных данных	
11	Уполномоченный представитель передающей стороны	Должность, ФИО, адрес электронной почты, телефон

3. Настоящим Стороны подтверждают, что документация (информация), указанная в пункте 1 настоящего акта, содержит конфиденциальную информацию, в связи с чем стороны обязуются выполнять в отношении такой информации обязательства, возложенные на них Соглашением.

4. На момент подписания настоящего акта Стороны друг к другу претензий не имеют.

5. Настоящий акт составлен в двух имеющих одинаковую юридическую силу экземплярах для каждой из Сторон.

6. МЕСТО НАХОЖДЕНИЯ, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Сторона – 1
(реквизиты Стороны)

_____ _____
(подпись) *(И.О.Фамилия)*

(печать)

Сторона – 2
(реквизиты Стороны)

_____ _____
(подпись) *(И.О.Фамилия)*

(печать)