

Приложение №1  
к Приказу № 36 от 19.08.2016 г.

**УТВЕРЖДАЮ**

Генеральный директор  
АО «НПФ «Стройкомплекс»



Орлова И.Ю.  
19.08.2016 г.

**ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**  
**АО «НПФ «СТРОЙКОМПЛЕКС»**

## **СОДЕРЖАНИЕ**

1. ОБЩИЕ ПОЛОЖЕНИЯ И ЦЕЛИ
2. ОБЛАСТЬ ДЕЙСТВИЯ
3. ПОЛИТИКА
4. ОТВЕТСТВЕННОСТЬ
5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

## 1. ОБЩИЕ ПОЛОЖЕНИЯ И ЦЕЛИ

1.1. Акционерное общество «Негосударственный пенсионный фонд «Стройкомплекс» (АО «НПФ «Стройкомплекс») (далее - Фонд) осуществляет свою деятельность по обязательному пенсионному страхованию и негосударственному пенсионному обеспечению, включая разработку и реализацию различных пенсионных программ. Осуществление указанной деятельности связано с накоплением, систематизацией и управлением информацией, в том числе и ограниченного доступа, являющейся важнейшим активом Фонда, и зависит от обеспечения информационной безопасности (далее - ИБ).

1.2. Политика ИБ (далее - Политика) Фонда является документом верхнего уровня и устанавливает высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, которыми Фонд руководствуется в своей деятельности, и направленные на:

- обеспечение непрерывности бизнес-процессов Фонда;
- обеспечение конфиденциальности, целостности и доступности информационных активов;
- минимизацию возможных потерь и ущерба от нарушений в области ИБ;
- достижение адекватности мер защиты существующим угрозам ИБ;
- поддержание положительной деловой репутации Фонда;
- повышение доверия к предлагаемым продуктам и услугам Фонда.

1.3. Для достижения указанных целей в Фонде внедряется Система обеспечения информационной безопасностью (далее - СОИБ), которая учитывает требования Федеральных законов Российской Федерации, нормативных правовых актов Правительства Российской Федерации, рекомендации и стандарты Банка России для некредитных финансовых организаций, а также требования и рекомендации государственных органов, уполномоченных в сфере ИБ.

1.4. Настоящая Политика является главным документом СОИБ для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения ИБ. Более подробное описание процедур организации СОИБ может быть описано в прочих внутренних документах Фонда (в том числе в частных Политиках) детализирующих положения настоящей Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Фонда в рамках организации СОИБ, разработанных с учетом данной Политики.

1.5. Разработка настоящей Политики, а также контроль за организацией, реализацией СОИБ и её соблюдением осуществляет подразделение (лицо), ответственное за информационную безопасность в Фонде, назначенное приказом Генерального директора Фонда.

## 2. ОБЛАСТЬ ДЕЙСТВИЯ

2.1. СОИБ, задокументированная в настоящей Политике, в частных Политиках, в Регламентах, в Правилах (процедурах), рабочих инструкциях и иных нормативных документах, является обязательными для исполнения всеми работниками Фонда (в том числе и временных работников) в области действия системы. Документированные требования СОИБ, а также все изменения в них, доводятся до сведения всех работников Фонда.

2.2. Требования настоящей Политики распространяются на всю информацию и ресурсы, участвующие в обработке информации в Фонде. Область действия частных Политик определены в самих частных Политиках.

## 3. ПОЛИТИКА

3.1. Фонду принадлежит на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в промышленную эксплуатацию в целях осуществления им деятельности в соответствии с действующим законодательством. Указанное право

собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования и каналов связи, предоставляемых Фондом, лицензионное и (или) разработанное (доработанное) программное обеспечение за счёт и в интересах Фонда, содержание ящиков корпоративной электронной почты в полном объеме, бумажные и электронные документы всех подразделений и работников Фонда. Работники Фонда получают доступ только к той информации, которая требуется для исполнения ими своих функциональных обязанностей.

3.2. Все частные Политики разрабатываются исходя из положения, что Фонд является самостоятельной организацией, а вся информация, принадлежащая Фонду, является его информационным активом. Фонд предпринимает меры для защиты своих информационных активов от несанкционированного использования, нарушения конфиденциальности, изменения или уничтожения. Вне зависимости от того, какие средства используются для создания, передачи или хранения информации, должны быть использованы адекватные меры по ее защите, определяемые Фондом самостоятельно.

3.3. Все материальные активы Фонда, включая аппаратное обеспечение, программное обеспечение, информационные ресурсы на бумажных и электронных носителях, а также персонал, подлежат учету.

3.4. Любая информация, принадлежащая Фонду, должна храниться и обрабатываться на рабочих станциях пользователей, серверах и электронных хранилищах данных, в том числе на отчуждаемых носителях информации (USB-накопители, внешние жёсткие диски HDD, переносные и мобильные устройства), принадлежащих Фонду.

3.5. В Фонде осуществляется регулярная оценка рисков ИВ. При ее проведении учитывается вероятность угроз ИВ и степень их влияния на бизнес-процессы и деловую репутацию Фонда.

3.6. По результатам оценки рисков ИВ выбираются и применяются средства управления для защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СОИБ.

3.7. Для обеспечения физической защиты информационных активов Фонда в границах области действия СОИБ устанавливаются зоны безопасности и принимаются меры для предотвращения неавторизованного доступа.

3.8. Фонд стремится выявлять, учитывать и реагировать на инциденты в сфере ИВ в соответствии с установленными процедурами.

3.9. В Фонде устанавливаются процедуры обеспечения непрерывности и восстановления деятельности критических бизнес-процессов.

3.10. Фонд проводит информирование, обучение и повышение квалификации работников в сфере ИВ.

3.11. В любых договорах с юридическими лицами, независимо от формы их организации, или физическими лицами, получающими доступ к любой информации Фонда, независимо от формы взаимодействия с ними, должна быть оговорена обязанность контрагента по соблюдению требований конфиденциальности информации, в том числе и при возникновении у них агентских правоотношений.

3.12. Настоящая Политика, частные Политики и иные документы СОИБ утверждаются (подписываются) Генеральным директором Фонда и должны быть доведены до каждого работника Фонда.

3.13. Настоящая Политика периодически пересматривается в случае изменений инфраструктуры фонда или существующих бизнес-процессов, а также в случае изменений в законодательстве в области ИБ, но не реже одного раза в два года.

#### **4. ОТВЕТСТВЕННОСТЬ**

4.1. Руководство Фонда осуществляет общее управление ИВ и обеспечивает необходимые условия для:

реализации мероприятий по оценке рисков ИВ и защиты информации;

поддержания, мониторинга, анализа и непрерывного улучшения СОИБ;

регулярного обучения работников Фонда в сфере ИБ,

4.2. Работники Фонда несут персональную ответственность за соблюдение требований документов СОИБ и обязаны сообщать обо всех выявленных нарушениях в области ИБ в подразделение (лицу), ответственному за информационную безопасность в Фонде. В

трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность и конфиденциальность информации, ставшей известной в силу выполнения ими своих обязанностей.

## **5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

5.1. Руководство Фонда заявляет своё одобрение настоящей Политики, которая объявлена, распространена, внедрена, доведена до всех работников и поддерживается на всех уровнях.

5.2. Настоящая Политика является общедоступным документом, который может предоставляться всем заинтересованным сторонам.

Прошито, пронумеровано и скреплено  
печатью С. Шевелев лист 26

Генеральный директор  
АО «НПФ «Строительский комплекс»  
Орловский филиал

