

Утверждаю
Директор Свердловского областного
фонда поддержки предпринимательства
_____ Копелян Е.А.
« _____ » _____ 2014 г.

Политика информационной безопасности

(редакция от 06.06.2014)

1. Свердловский областной фонд поддержки предпринимательства (далее – Фонд) – региональный институт развития, созданный в 2002 году Правительством Свердловской области в целях развития малого и среднего бизнеса Свердловской области.
2. Осуществление Фондом уставной деятельности связано с управлением информацией, являющейся важным активом Фонда, и зависит от обеспечения информационной безопасности, под которой понимается обеспечение конфиденциальности, целостности и доступности информационных активов.
3. Политика информационной безопасности Фонда устанавливает цели, задачи и подходы в области информационной безопасности, которыми Фонд руководствуется в своей деятельности.
4. Политика информационной безопасности Фонда распространяется также на организации и граждан, уполномоченных Фондом реализовывать отдельные его функции на территориях муниципальных образований Свердловской области.
5. Политика информационной безопасности Фонда направлена на достижение следующих целей:
 - обеспечение безопасности и конфиденциальности персональных данных и иной информации с ограниченным доступом;
 - обеспечение непрерывности основных бизнес-процессов Фонда;
 - минимизация возможных потерь и ущерба от нарушений в области информационной безопасности.
6. Для достижения указанных целей в Фонде внедряется Система управления информационной безопасностью, соответствующая:
 - международному стандарту ISO/IEC 27001:2005;
 - требованиям законодательства Российской Федерации и договорным обязательствам Фонда в области информационной безопасности.
7. Фонд обеспечивает разработку, внедрение и исполнение документов, регламентирующих деятельность Фонда в области обеспечения информационной безопасности:
 - документ по информационной безопасности первого уровня – настоящая Политика информационной безопасности СОФПП, распространяется на всех сотрудников Фонда;
 - документы по информационной безопасности второго уровня – Положение о системе управления информационной безопасностью СОФПП и Положение о конфиденциальной информации СОФПП, распространяются на всех сотрудников Фонда;
 - документы по информационной безопасности третьего уровня - правила, регламенты, рабочие инструкции, которые распространяются на всех или на явно указанных в данных документах группы сотрудников Фонда.

8. Все информационные активы Фонда, включая информационные ресурсы на бумажных и электронных носителях, а также аппаратное обеспечение, программное обеспечение, персонал, подлежат учету и категорированию в соответствии с их важностью и степенью доступа.

9. Фонд разрабатывает и обеспечивает регулярное проведение процедур оценки рисков информационной безопасности. При оценке рисков должна учитываться вероятность угроз информационной безопасности и степень их влияния на бизнес-процессы, финансовое состояние и деловую репутацию Фонда.

По результатам оценки рисков информационной безопасности выбираются и применяются организационные, физические, технические, программные и программно-аппаратные средства обеспечения информационной безопасности.

10. Фонд обеспечивает физическую защиту информационных активов Фонда в административном здании Фонда, расположенном по адресу: г. Екатеринбург, ул. Восточная, 7д, а также налагает на организации, реализующие отдельные функции Фонда в муниципальных образованиях Свердловской области, обязательства по обеспечению защиты информационных активов Фонда в занимаемых ими помещениях. Для этого устанавливаются зоны безопасности и принимаются меры для предотвращения неавторизованного доступа.

11. Фонд обязуется выявлять, учитывать и реагировать на инциденты в сфере информационной безопасности в соответствии с установленными процедурами.

12. В Фонде разрабатываются и внедряются процедуры обеспечения непрерывности критических бизнес-процессов от эффектов существенных сбоев информационных систем или чрезвычайных ситуаций, процедуры контроля работоспособности средств обеспечения информационной безопасности.

13. Работникам Фонда и представительств Фонда предоставляется доступ к той информации, которая требуется для исполнения их функциональных обязанностей.

14. Фонд проводит информирование, обучение и повышение квалификации работников в сфере информационной безопасности.

15. Работники Фонда и уполномоченные действовать от имени Фонда лица и организации обязаны соблюдать требования документов по информационной безопасности, в том числе обеспечивать сохранность служебной документации и конфиденциальность информации, ставшей известной в силу выполнения ими своих обязанностей, а также сообщать обо всех выявленных нарушениях в области информационной безопасности руководству Фонда.

В трудовых договорах работников Фонда и договорах, уполномочивающих лиц и организации действовать от лица Фонда, устанавливается ответственность за несоблюдение требований документов по информационной безопасности.

16. Руководство Фонда осуществляет общее управление информационной безопасностью Фонда и обеспечивает необходимые условия для:

- поддержания, мониторинга, анализа и непрерывного улучшения системы управления информационной безопасностью;
- реализации мероприятий по оценке рисков информационной безопасности и защиты информации;
- обучения работников Фонда и представительств Фонда в сфере информационной безопасности.

17. Политика информационной безопасности Фонда является общедоступным документом, который может предоставляться всем заинтересованным сторонам и размещается на официальном веб-сайте Фонда.

Лист согласования

(Политика информационной безопасности, ред. от 06.06.2014)

ФИО	Должность	Подпись	Дата
Пиличев Валерий Валерьевич	Заместитель директора		
Сулла Илья Иосифович	Заместитель директора		
Томин Олег Петрович	Заместитель директора		
Балашова Анна Сергеевна	Юрист		