**ГЛАВА ГОРОДСКОГО ПОСЕЛЕНИЯ «ГОРОД БИКИН»**

**Бикинского муниципального района хабаровского края**

**РАСПОРЯЖЕНИЕ**

12.08.2011 №256-р

Об утверждении Положения

о парольной защите при

обработке персональных

данных и иной

конфиденциальной информации

# Руководствуясь требованиями Федерального закона от 27.07.2006  № 152-ФЗ «О персональных данных» (в ред. от 25.07.2011 №261-ФЗ), Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и иных нормативных правовых актов в сфере защиты информации,

1. Утвердить прилагаемое Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации (далее - Положение).

2. Общему отделу администрации городского поселения (Коростинская Т.Д.) довести Положение до сведения руководителей структурных подразделений, где осуществляется обработка персональных данных и иной конфиденциальной информации, а также до сведения Пользователей, допущенных к обработке персональных данных и иной конфиденциальной информации.

3. Специалисту по оказанию консультационных услуг по программным средствам обслуживания вычислительной техники Николишину Д.О. (по согласованию) обеспечить режим парольной защиты при обработке персональных данных и иной конфиденциальной информации в соответствии с утверждённым Положением.

4.Настоящее распоряжение вступает в силу со дня его подписания.

И. о. главы администрации

городского поселения Э.Ю. Бордовский

УТВЕРЖДЕНО

распоряжением

администрации

городского поселения

«Город Бикин»

от\_12.08.2011 №256-р\_\_\_\_

ПОЛОЖЕНИЕ

о парольной защите при обработке персональных данных и иной конфиденциальной информации

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (учетных записей Пользователей) в информационных системах (ИС) администрации городского поселения «Город Бикин» (далее - Оператора), а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех ИС и контроль за действиями Пользователей и обслуживающего персонала при работе с паролями возлагается на специалиста по оказанию консультационных услуг по программным средствам обслуживания вычислительной техники.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее 8 символов;
* в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.);
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
* при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
* личный пароль Пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на специалиста по оказанию консультационных услуг по программным средствам обслуживания вычислительной техники.

Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления с паролями других сотрудников подразделений Оператора.

4. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей передавать на хранение руководителю своего подразделения их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте.

5. Полная смена паролей Пользователей должна проводиться не реже одного раза в полгода.

6. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного Пользователя с системой.

7. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) специалиста по оказанию консультационных услуг по программным средствам обслуживания вычислительной техники и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п. 6 или п. 7 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение Пользователем своих паролей на бумажном носителе допускается только в сейфе.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_