***Приложение 1***

к Договору оферты

«Условия дистанционного банковского обслуживания

юридических лиц и индивидуальных предпринимателей

 в Банке РМП (ПАО) с использованием системы

«Мобильный банк для юридических лиц»

**Рекомендации по обеспечению безопасности мобильных устройств**

1. Используйте только официальные магазины приложений, контролирующие размещаемые приложения на предмет наличия вредоносного кода. Не устанавливайте приложения из сомнительных или непроверенных источников.
2. Минимизируйте число установленных приложений на вашем мобильном устройстве.
3. Контролируйте предоставляемые приложениям права на доступ к функциям и информации на мобильном устройстве, не предоставляйте приложениям права доступа не требуемые для их работы (например, для программы просмотра изображений или приложения «Фонарик» доступ к СМС-сообщениям будет избыточным).
4. Установите и используйте антивирусное приложение известного производителя средств защиты от вредоносного кода (антивирусных средств).
5. Используйте надежные пароли и PIN-коды, периодически их меняйте, установите PIN-код на SIM-карту. Пароли и PIN-коды не должны содержать даты значимых для вас событий (или их части, например – день и месяц), части номеров сотовых и городских телефонов вас и ваших близких, простых последовательностей цифр (12345, 0001, 0002, 1111, 2222, 0987 и т.п.).
6. Старайтесь не использовать бесплатные, общедоступные точки доступа и обращайте внимание на результаты проверки сертификата при HTTPS соединении – есть вероятность перехвата и раскрытия передаваемых данных или взлома вашего мобильного устройства злоумышленниками.
7. Отключите для уведомлений на мобильном устройстве показ текста сообщения, чтобы предотвратить возможность ознакомления злоумышленников с кодами подтверждения операций.
8. Учетная запись, к которой привязано ваше мобильное устройство, должна контролироваться вами или вашей организацией, чтобы предотвратить возможность прямого или косвенного удаленного доступа к вашему устройству.