**УТВЕРЖДАЮ**
**Заместитель директора Департамента информатизации Тюменской области**

_____**С.И. Логинов**
«__15__» ____10_____ **2019 г.**

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

## ПОЛИТИКА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ

ОИБ-ТО/3.13/005

Тюмень, 2019 г.

## 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины, определения и сокращения, применяемые в настоящем документе, используются в соответствие с документом №ОИБ-ТО/3.13/001 «Термины и определения».

## 2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1. Настоящий документ (далее — Политика) определяет требования информационной безопасности при использовании электронных почтовых систем в рамках государственной сети передачи данных Правительства Тюменской области (далее — ГСПД ТО).

2.2. Настоящая Политика:

- определяет порядок организации и использования электронной почты в ГСПД ТО;
- обязательна для исполнения всеми сотрудниками организаций — Участниками процессов ИБ, партнерами и третьими сторонами, использующими почтовые системы ГСПД ТО;
- обязательна для исполнения всеми контрагентами, имеющими подписанные Соглашения или Договоры об использовании услуги серверов электронной почты, в части их касающейся;
- используется при проектировании, построении и эксплуатации систем электронной почты, а также служит руководством для написания Инструкции, Регламентов и Процедур, описывающих порядок предоставления и использования услуги.

2.3. Политика подлежит пересмотру с периодичностью 1 раз в год для приведения системы защиты в соответствие реальным условиям. Также может проводиться внеплановый пересмотр при изменении перечня решаемых задач, конфигурации технических и программных средств, а также при изменении требований законодательства в области информационной безопасности.

## 3. ОБЩИЕ ТРЕБОВАНИЯ

3.1. В ГСПД ТО созданы и эксплуатируются почтовые ресурсы и системы, предназначенные для обеспечения обмена электронной почтой между Участниками процессов ИБ и внешними почтовыми системами, в том числе международными.

3.2. Услуга электронной почты на серверах ГСПД ТО может быть предоставлена другим государственным учреждениям и коммерческим организациям. Условия предоставления услуги оговариваются и закрепляются в соответствующих соглашениях или договорах.

3.3. Оператор почтовой системы поддерживает необходимый уровень безопасности и надежности доставки электронной почты внутри ГСПД ТО, и другим лицам через внешние сети (по отношению к ГСПД ТО).

## 4. ТРЕБОВАНИЯ К СЕРВЕРАМ ПОЧТОВЫХ СИСТЕМ

4.1. Сервера почтовых систем, как часть информационных ресурсов ГСПД ТО, должны защищаться в соответствии с необходимым классом защищенности.

4.2. Все почтовые сообщения, проходящие через сервера почтовых систем ГСПД ТО, должны проверяться антивирусным программным обеспечением, блокирующим распространение и передачу вредоносного программного обеспечения.

4.3. Все почтовые сообщения, проходящие через сервера почтовых систем ГСПД ТО, должны проверяться на подлинность отправителя сообщения. Сообщения, не прошедшие проверку подлинности отправителя блокируются.

4.4. На серверах почтовых систем должно проводится регулярное резервное копирование сообщений электронной почты, системных и пользовательских данных. Оперативное восстановление случайно (намеренно) удаленных почтовых сообщений осуществляется в течение 14 дней с момента удаления (за исключением сообщений, хранящихся на локальных компьютерах пользователей - такие сообщения восстановление не подлежат). При необходимости восстановления писем, удаленных ранее этого срока запускается процедура восстановления писем, удаленных ранее этого срока запускается процедура восстановления данных из резервной копии, описанная в соответствующем Регламенте.

4.5. Регламенты технического обслуживания серверов почтовых систем разрабатываются организацией - Оператором почтовой системы.

4.6. На всех серверах почтовых систем должно проводиться журналирование системных событий и ошибок. Журналы сообщений должны защищаться от несанкционированного просмотра, модификации или уничтожения. Срок хранения журналов доставки - не более 30 дней.

4.7. Все сервера почтовых систем должны иметь назначенных администраторов, отвечающих за функциональность, безопасность и работоспособность серверов. На администраторов серверов возлагается обязанность регистрации и смены идентификационных данных пользователей в соответствии с действующими Процедурами.

4.8. Внутренние сервера почтовых систем должны быть отделены от внешних сетей с применением сетевых технических средств и межсетевого экранирования, находиться в пределах демилитаризованной зоны (и/или контролируемой зоны). Обмен сообщениями и служебной информацией между внутренними и внешними серверами почтовых систем осуществляется через контролируемые точки доступа.

## 5. ТРЕБОВАНИЯ К СЕРВИСУ ЭЛЕКТРОННОЙ ПОЧТЫ

5.1. Сервис электронной почты для сотрудников Участников процессов ИБ (далее – сотрудники) предназначен для ведения служебной или деловой переписки, использования в технологических процессах. Использование в личных целях запрещено.

5.2. За каждым сотрудником, использующим сервис электронной почты, закрепляется свой персональный адрес корпоративной электронной почты или список адресов, персональный адрес создается в формате ФамилияИО@имя_домена.

5.3. Запрещено использование чужих идентификационных данных при пользовании сервисом электронной почты.

5.4. Запрещено использование сервиса электронной почты для приема или передачи сообщений, содержащих исполняемые файлы.

5.5. Передача сообщений через сервис электронной почты разрешена только с обязательной аутентификацией на почтовых серверах.

5.6. Запрещается создание идентификационных записей для сторонних пользователей или пользователей внешних сетей на внутренних серверах почтовых систем.

5.7. Запрещается использование сервиса электронной почты в целях и формах, противоречащих действующему законодательству и иным нормативным актам Российской Федерации или не соответствующих общепринятым правилам этики в том числе кодексу профессиональной этики государственных гражданских служащих Тюменской области, утвержденного распоряжением Губернатора Тюменской области от 25 апреля 2011г. №23-р.

5.8. Доступ к справочнику адресов электронной почты, используемых сотрудниками в служебных целях, подлежит ограничению в соответствии с положениями Федерального закона 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

5.9. Служебные учетные записи, создаваемые в технологических целях для автоматической рассылки или обработки сообщений программными средствами, не должны предоставлять возможности регистрации пользователей с идентификационными данными указанных учетных записей.

5.10. Сотрудникам запрещается осуществлять автоматическую пересылку и хранение служебных почтовых сообщений на внешних серверах почтовых систем и ресурсах внешних сетей.

5.11. Уполномоченный орган оставляет за собой право ведения мониторинга, протоколирования и проведения выборочных проверок характера использования сервиса электронной почты сотрудниками.

5.12. Уполномоченный орган оставляет за собой право ограничивать сотрудникам доступ из ГСПД ТО к почтовым ресурсам, расположенным во внешних сетях.

5.13. Схема организации почтового сервиса должна поддерживать:

- антивирусный контроль передаваемых сообщений;
- фильтрацию нежелательных сообщений (спама);

- непрерывность предоставления сервиса;
- фильтрацию сообщений по произвольным критериям;
- архив почтовых сообщений;
- возможность шифрования сообщений электронной почты;
- возможность удостоверения сообщений электронной почты электронно-цифровой подписью;
- масштабируемость сервиса, как по количеству передаваемых сообщений, так и по количеству пользователей.

5.14. Запрещено использование сервиса электронной почты для передачи сообщений, содержащих информацию ограниченного доступа.

## 6. ОТВЕТСТВЕННОСТЬ

6.1. Ответственность за функциональность и работоспособность серверов почтовых систем возлагается на Оператора почтовой системы.

6.2. Ответственность за сохранность и конфиденциальность персональных идентификационных данных пользователей сервисом электронной почты возлагается персонально на каждого пользователя и уполномоченных сотрудников, осуществляющих их регистрацию.

6.3. Сотрудники пользующиеся сервисом электронной почты, руководствуются настоящими Правилами и несут персональную ответственность за исполнение их требований, а также требований других действующих регламентирующих документов.

6.4. Пользователи услуги электронной почты из числа сотрудников партнеров (контрагентов) несут ответственность за правильность и правомерность использования услуги в соответствии с действующими Соглашениями или Договорами, а так же действующим законодательством РФ.

6.5. Нарушение политики, не ставшее причиной и не повлекшее за собой разглашения информации, является основанием для привлечения виновных сотрудников к дисциплинарной ответственности.

6.6. Разглашение информации или ее использование в целях, не связанных с исполнением должностных обязанностей, является основанием для привлечения к дисциплинарной, гражданско-правовой, а также к административной или уголовной ответственности.

**История изменений.**

| № п/п | Версия, дата документа | Автор | Примечания |
|---|---|---|---|
| 1 | Версия 1.0 от 19.07.2013 | Островский С.В. | Введен впервые |
| 2 | Версия от 20.07.2015 | Овсянко А.Г. | - |
| 3 | Версия от 06.02.2017 | Забокрицкий А.О. | - |
| 4 | Версия от 01.06.2017 | Кичигина А.А. | - |
| 5 | Версия от 07.10.2019 | Бею Д.Н. | - |