УТВЕРЖДАЮ
Директор ГПОАУ АТК
_____Кривцов О.А.
«___»_____ 2018 г.

ПОЛОЖЕНИЕ
о порядке доступа к ресурсам серверов
ГПОАУ «Амурский технический колледж»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее положение устанавливает порядок доступа к ресурсам серверов ГПОАУ АТК (далее – Сервисам) сотрудниками Государственного профессионального образовательного автономного учреждения Амурской области «Амурский технический колледж» (далее по тексту – ГПОАУ АТК).

1.2. Настоящее положение имеет статус локального нормативного акта ГПОАУ АТК, регламентирующего использование Сервисов. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящим Положением, применяются нормы действующего законодательства.

1.3. Порядок доступа к Сервисам разработан во исполнение и с учетом требований и положений следующих нормативных документов:

- Федерального закона Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- Федерального закона «Об информации, информационных технологиях и о защите информации» от 26.07.2006 № 149-ФЗ;
- Инструкции о мерах по обеспечению безопасности информационной системы ГПОАУ АТК.

2. ОСНОВНЫЕ ТЕРМИНЫ, СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения служебных обязанностей.

Доступ к информации - возможность получения информации и ее использования.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Локальная сеть - коммуникационная система, состоящая из нескольких компьютеров, соединенных между собой посредством кабелей (телефонных линий, радиоканалов), позволяющая пользователям совместно использовать ресурсы компьютера: программы, файлы, папки, а также периферийные устройства.

Пароль — секретный набор символов (букв, цифр, специальных символов), предъявляемый пользователем компьютерной системе для получения доступа к данным и программам.

Пользователь – сотрудник организации, использующий АРМ, для выполнения своих должностных обязанностей.

Сервер — аппаратно-программный комплекс, выполняющий определенные задачи для групп электронных устройств.

Системный администратор — должностное лицо, в обязанности которого входит обслуживание всего аппаратно-программного комплекса организации, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных, их резервное копирование и восстановление.

3. ПОРЯДОК ИСПОЛЬЗОВАНИЯ СЕРВИСОВ

3.1. Порядок применяется во всех случаях, когда пользователям ГПОАУ АТК или пользователям сторонних организаций, выполняющим работы на территории и с использованием технических средств ГПОАУ АТК, предоставляется (впервые или по истечении срока предыдущего получения аналогичных прав доступа) доступ к Сервисам.

3.2. На АРМ, использующем Сервисы, в обязательном порядке должно быть установлено антивирусное программное обеспечение с актуальной антивирусной базой.

3.3. Доступ к Сервисам предоставляется ограниченному кругу Пользователей в целях выполнения ими своих служебных обязанностей после ознакомления с настоящим Положением. Для доступа к Сервисам пользователь должен ввести свои регистрационное имя и пароль, полученные у системного администратора.

3.4. Пользователи обязаны незамедлительно сообщать системному администратору о замеченных случаях нарушения компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации).

3.5. Пользователям запрещается:

3.5.1. Подключать к локальной сети ГПОАУ АТК новые компьютеры и оборудование без участия системного администратора.

3.5.2. Передавать другим лицам свои личные атрибуты доступа (регистрационное имя и пароль) к компьютерному оборудованию и Сервисам.

3.5.3. Осуществлять доступ к оборудованию и Сервисам с использованием чужих личных атрибутов доступа или с использованием чужого сеанса работы.

3.5.4. Удалять файлы других пользователей на серверах общего пользования.

3.5.6. Осуществлять попытку несанкционированного доступа к компьютерному оборудованию и информации хранящейся на компьютерах и передаваемой по сети.

3.5.7. Использовать, распространять и хранить программы, предназначенные для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерные вирусы и любые программы ими инфицированные.

3.5.8. Предоставлять доступ к компьютерному оборудованию незарегистрированным пользователям.

3.5.9. Хранить незащищенную от несанкционированного доступа информацию, содержащую персональные данные, на серверах общего пользования.

3.5.10. Хранить защищенные авторскими правами материалы на серверах общего пользования, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ними права третьей стороны.

3.5.11. Выполнять действия и команды, результат и последствия которых пользователю не известен.

3.5.12. Оставлять без присмотра незаблокированное АРМ.

3.6. Пользователи имеют право:

3.6.1. Подавать заявку на получение права доступа к Сервисам.

3.6.2. Вносить предложения по установке бесплатного и приобретению коммерческого программного обеспечения общего пользования.

3.6.3. Вносить предложения по улучшению настроек оборудования и программного обеспечения общего пользования.

3.6.4. Получать консультацию у системного администратора по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности.

3.7. Правила использования и хранения паролей:

3.7.1. При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.).

3.7.2. Запрещается хранить пароли на бумаге, в файлах и других носителях информации, в том числе на предметах, непосредственно на рабочем месте пользователя.

3.7.3. Носители с записями паролей должны храниться в надежном и доступном только владельцу месте.

3.7.4. Пользователям запрещается действием или бездействием способствовать разглашению своего пароля.

3.7.5. Запрещается сообщать пароли другим пользователям и регистрировать их в системах под своей учетной записью, за исключением случаев устранения неисправностей (в присутствии пользователя).

3.7.6. Запрещается пересылать пароль открытым текстом в сообщениях электронной почты.

3.7.8. В случае утери или компрометации пароля пользователь обязан незамедлительно предпринять меры по смене пароля: сменить его самостоятельно, либо оформить заявку на смену пароля в адрес системного администратора.

3.8. Обязательным является соблюдение конфиденциальности информации, хранимой на АРМ и серверах ГПОАУ АТК, доступ к которой ограничен федеральными законами.

3.9. Запрещается распространение и хранение информации на АРМ и Сервисах ГПОАУ АТК, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

3.10. В случае нарушения пунктов Положения системный администратор ГПОАУ АТК вправе аннулировать доступ пользователя к Сервисам, уведомив об этом руководство структурного подразделения.

4. ОТВЕТСТВЕННОСТЬ

4.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами ГПОАУ АТК.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Анализ актуальности данного Положения должен проводиться системным администратором ГПОАУ АТК не реже одного раза в год, а также в каждом случае внедрения новых сервисов в дополнение к имеющимся. В случае если в ходе такого анализа была установлена необходимость внесения изменений в Положение, новая редакция Положения должна быть утверждена приказом по ГПОАУ АТК.

5.2. Контроль над соблюдением требований данного Положения проводится системным администратором ГПОАУ АТК.