Информационная безопасность

Правила пользования ресурсами корпоративной сети Компании

Обеспечение информационной безопасности - необходимое условие осуществления деятельности Компании.
Нарушение информационной безопасности может привести к серьезным негативным последствиям, включая прямой материальный ущерб, потерю доверия со стороны клиентов и снижение конкурентоспособности.
Вся информация, хранимая, обрабатываемая и передаваемая по каналам связи в корпоративной сети Компании, которая не была специально идентифицирована как собственность третьих сторон, - собственностью Компании.
Регламент информационной безопасности запрещает несанкционированный доступ, раскрытие, дублирование, изменение, удаление, ненадлежащее использование информации, а также хищение носителей этой информации.

Первоначальный доступ к ресурсам корпоративной сети предоставляется сотруднику Компании в соответствии с его служебными обязанностями.
Пользователь имеет право приступить к работе в корпоративной сети только после ознакомления с документами, регламентирующими правила работы пользователей в корпоративной сети.
На основании заявки непосредственного руководителя (или уполномоченного им лица), направляемой в службу Service Desk, согласно внутренней процедуры SD формируются запросы на предоставление доступа к указанным в заявке информационным ресурсам компании и направляются специалистам в профильных подразделениях.

Подключение к корпоративной сети Компании

В Компании существует корпоративная сеть и

и Пользователь имеет право приступить к работе в корпоративной сети только после ознакомления с документами, регламентирующими правила работы пользователей в корпоративной сети.
На основании заявки непосредственного руководителя (или уполномоченного им лица), направляемой в службу Service Desk, согласно внутренней процедуры SD формируются запросы на предоставление доступа к указанным в заявке информационным ресурсам компании и направляются специалистам в профильных подразделениях.

Общие требования безопасности, предъявляемые к пользователям корпоративной сети

Пользователь не должен читать, изменять, удалять или копировать любые файлы, принадлежащие другим пользователям, не получив предварительно разрешения от владельца файла. Если явно не установлен доступ для всех пользователей, как это имеет место в совместно используемых каталогах, возможность считывать, изменять, удалять или копировать файлы, принадлежащие другим пользователям, не означает разрешения на выполнение этих действий.

Пользователям запрещается использовать ресурсы корпоративной сети Компании для получения несанкционированного доступа к любым другим сетям (системам), не принадлежащим Компании, или каким-либо образом создавать помехи, изменять либо нарушать функционирование этих систем. Более того, сотрудникам запрещается предпринимать действия для получения паролей, ключей шифрования и любых других данных, которые могут быть использованы для получения несанкционированного доступа к информационным ресурсам корпоративной сети Компании.

Пользователи должны выбирать надежные пароли, не сообщать их другим лицам, соблюдать правила их хранения, использования и периодичности смены в соответствии с требованиями «Регламента управления паролями».

Пользователь несет личную ответственность за сохранение данных на локальных жестких дисках персональных компьютеров. Сотрудниками Департамента Информационных Технологий (далее ДИТ) сохранность этих данных не гарантируется. Всю служебную информацию пользователь должен хранить на специальных файловых серверах, для которых производится резервное копирование.

Оставляя свое рабочее место без присмотра (независимо от времени отсутствия), работник должен заблокировать на компьютере «Рабочий стол» нажатием на компьютерной клавиатуре набора клавиш Ctrl+Alt+Del и далее - кнопки «Блокировка» («Lock Workstation»).

Пользователям запрещено

- портить наклейку или делать нечитаемой информацию, подтверждающую подлинность установленного на компьютере программного обеспечения;
- самостоятельно устанавливать нелицензионное программное обеспечение;
- самостоятельно устанавливать, деинсталлировать и модифицировать программное обеспечение, изменять текущие настройки операционной системы и ПО (за исключением пользователей, которым Администратором сети в настройках компьютерных систем предоставлены соответствующие полномочия);
- самостоятельно ремонтировать, разбирать или изменять конфигурацию компьютеров, принтеров и др. компьютерного оборудования;
- нарушать правила эксплуатации компьютерного оборудования, загораживать вентиляционные отверстия, проливать жидкости на клавиатуру, корпус компьютера и монитор, наклеивать картинки и другие аппликации на монитор и корпус компьютера (за исключением специально предназначенных для этого «бумаг для заметок»);
- предоставлять доступ к локальным ресурсам своего компьютера другим лицам без разрешения Администратора сети и без согласования с ДЭБ;
- самостоятельно перемещать оборудование в пределах рабочего места, с одного рабочего места на другое или между офисами;
- преднамеренно записывать, создавать, компилировать, копировать, распространять, запускать на выполнение или пытаться встраивать любые машинные коды, разработанные для самовоспроизводства, повреждения или создания иных помех функционированию ИС Компании и нормальной работе других пользователей;
- производить останов или отключение этих антивирусных средств.
- Пользователям запрещается осуществлять массовую почтовую

Доступ к ресурсам сети Интернет и работа с электронной почтой

При работе в сети Интернет и с системой электронной почты сотрудник, имеющий возможность отправки электронных писем, лично отвечает за соблюдение коммерческой тайны предприятия.

При приеме электронных писем сотрудник обязан при помощи штатных антивирусных средств, предоставляемых Компанией, проверить, что в присланной корреспонденции не содержится вирусов, способных нарушить работу компьютеров и сети. В случае получения корреспонденции сомнительного содержания, либо от неизвестного адресата, пользователь немедленно обязан сообщить об этом системному администратору, самостоятельно не предпринимая никаких действий.

Пользователь должен стремиться оптимально использовать канал доступа в Интернет. При несоблюдении настоящих требований по работе в сети Интернет сотрудник может быть временно или постоянно отключен от ресурсов Интернет.

Для осуществления как внутренних, так и внешних обменов сообщениями электронной почты пользователь обязан пользоваться штатными средствами, предоставляемыми ДИТ. Без предварительного разрешения руководителя своего структурного подразделения и ДЭБ сотрудникам запрещается использовать для передачи сообщений, касающихся деятельности Компании, системы электронной почты, предоставляемые Интернет-провайдерами или иными нештатными средствами (например, общедоступными почтовыми серверами, такими как www.mail.ru, www.hotmail.ru и т.п.).

Ответственность сотрудников Компании

За соблюдение Правил работы в корпоративной сети Компании пользователь несет персональную ответственность. В случае нарушения настоящих Правил Пользователь может быть ограничен в правах доступа к ресурсам корпоративной сети, либо временно отключен от сетевых ресурсов.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования корпоративной политики безопасности, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный компании в результате нарушения ими правил настоящей политики (Ст. 238 Трудового кодекса РФ) в пределах, установленных действующим законодательством. Под прямым действительным ущербом, в данном случае, понимается необходимость для Компании произвести затраты либо излишние выплаты на приобретение или восстановление данных. Сотрудник Компании также несет материальную ответственность за ущерб, возникший у работодателя в результате возмещения им ущерба иным лицам.

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники Компании несут материальную ответственность в полном размере причиненного ущерба (Ст. 243 Трудового кодекса РФ).

Возмещение ущерба производится независимо от привлечения сотрудника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб Компании (Ст. 248 Трудового кодекса РФ).