

Инструкция по

- использованию и контролю за использованием сети Интернет, электронной почтой и телефонными разговорами, а также**
- проверка учетной записи сотрудника**

29 августа 2013 г.

Содержание

Введение.....	3
1. Использование интернет-сервисов и телефонных служб	3
2. Контроль за использованием интернет-сервисов и телефонных служб	3
2.1 Протоколирование.....	3
2.2 Запрет на шпионские программы	4
2.3 Обработка результатов протоколирования	4
2.4 Контроль в рамках гарантии надежности и функциональности производственной системы электронной обработки данных	4
2.5 Продолжительность хранения	4
3. Разграничение личной и деловой электронной почты	4
4. Санкции при нарушениях.....	5
5. Управление электронной почтой при отсутствии/уходе сотрудника	5
5.1 Ожидаемое отсутствие	5
5.2 Непредвиденное отсутствие	5
5.3 Непредвиденное продолжительное отсутствие	5
5.4 Уход сотрудника	5
6. Инспекция учетной записи сотрудника	6
7. Подозрение в преступном поведении.....	6
8. Информация.....	7
9. Вступление в силу	7
Приложение: Бланк заявления на получение права инспекции учетной записи сотрудника	8

Введение

Данная инструкция устанавливает правила использования интернет-сервисов и телефонных служб сотрудниками компаний концерна AFG Arbonia-Forster-Holding AG (далее — AFG). Кроме того, назначением данной инструкции является защита сотрудников и компании AFG при контроле этих служб и проверке учетной записи. Следует соблюдать местные предписания, которые предполагают более серьезные правила или используются при приведении в исполнение данной инструкции.

1. Использование интернет-сервисов и телефонных служб

Каждому сотруднику предоставляется возможность использования интернет-сервисов (Интернет, электронная почта) с индивидуальным паролем. Использование этих сервисов, а также телефонных служб должно в первую очередь служить бизнес-целям и позволяет лучше и/или рациональнее или профессиональнее выполнять работу.

Применение доступных интернет-сервисов и телефонных служб в первую очередь предназначено для целей предприятия. Допускается их использование в личных целях во время пауз и в очень ограниченном количестве.

Запрещается посещать страницы с криминальным, порнографическим и расистским содержанием. Кроме того, запрещено участие в соответствующей деятельности (например, путем обмена мнениями в чатах, по электронной почте и т. д.). Автоматические фильтры блокируют страницы определенных категорий. Для всех сотрудников заблокированы страницы со следующим содержанием: порнография, криминальные действия, экстремистское содержание, веб-радио, чаты, наркотики.

Из соображений безопасности все электронные письма и выходы в Интернет, в том числе загрузки, автоматически проверяются на вирусы и при необходимости блокируются. Несмотря на это, сотрудникам следует немедленно удалять электронные письма от неизвестных отправителей или письма, в которых есть подозрение на наличие вируса, не открывая и не читая их. Сообщения в Интернете как правило квитируются нажатием кнопки «Нет» или «Отмена». Ни в коем случае не открывайте и не скачивайте вложения в письмах от неизвестных отправителей.

Все зашифрованные входы в Интернет (например, онлайн-банкинг) раскодируются и также автоматически проверяются.

2. Контроль за использованием интернет-сервисов и телефонных служб

2.1 Протоколирование

Отдел информационных технологий протоколирует все виды интернет-активности. Входящие и исходящие звонки протоколируются операторами телефонной сети. Под протоколированием понимается постоянная регистрация основных данных «кто», «что», «когда», которая в концерне AFG проводится в следующих случаях:

- Интернет (посещенные страницы, пользователь, дата, время),
- электронная почта (отправитель, получатель, дата, время, строка темы),
- регистрация в системе (пользователь, дата, время),
- телефон (телефонные номера всех участников разговора, время, дата, продолжительность).

2.2 Запрет на шпионские программы

Запрещается использовать шпионские программы.

2.3 Обработка результатов протоколирования

Обработка результатов протоколирования происходит на различных уровнях.

Анонимная обработка Анонимная обработка предназначена для составления статистики, например, для структурированной демонстрации среднестатистического использования сети Интернет, самых посещаемых страниц и т. д. Количество анализируемых пользователей должно быть достаточно большим, чтобы невозможно было выявить отдельных сотрудников (например, все сотрудники компании AFG Management AG).

Персонализированная обработка Персонализированная обработка разрешается только в том случае, если при анонимной обработке были выявлены нарушения или возникло подозрение в таком нарушении. Нарушением считается невыполнение пользовательских предписаний из пункта 1 данной инструкции или других обязательств согласно трудовому договору.

Персонализированная обработка проводится по заявке руководителя и выполняется ответственным отделом кадров в сотрудничестве с отделом информационных технологий и, при его наличии, с уполномоченным лицом по защите данных. Если подозрение в нарушении не подтверждается, обработка личных данных немедленно прекращается, а поднятые данные уничтожаются.

2.4 Контроль в рамках гарантии надежности и функциональности производственной системы электронной обработки данных

В случае возникновения неисправностей в системе электронной обработки данных, несмотря на технические средства защиты, для поиска их причины разрешается привлекать протоколы. Если выясняется, что причиной неисправности является нарушение правил, виновный сотрудник может быть подвергнут санкциям согласно пункту 4 данной инструкции.

2.5 Продолжительность хранения

В целях обеспечения доказательств протоколы интернет-активности хранятся в течение четырех недель, однако если того требует процедура применения санкции или уголовное производство, срок хранения может быть продлен. Хранение протоколов телефонных разговоров зависит от местных правовых норм, касающихся телефонных разговоров.

3. Разграничение личной и деловой электронной почты

Учетная запись электронной почты предназначена прежде всего для целей предприятия. Личные письма следует максимально ограничить. Компания AFG не просматривает и не обрабатывает электронные письма, обозначенные как личные. Если письмо никак не отмечено как личное, и его природа не устанавливается на основе элементов адресации или другим способом, AFG может исходить из того, что данное письмо является служебным. При возникновении сомнений по поводу природы письма следует прояснить этот вопрос с сотрудником.

Служебные письма при необходимости можно защитить.

Как только выясняется, что письмо личное, AFG не имеет права ознакомляться с его содержанием. Это правило действует и в том случае, если путем электронной почты было совершено преступление или другое нарушение согласно пункту 1 данной инструкции.

4. Санкции при нарушениях

Если предпосылки и правила контроля были соблюдены, и при этом установлен факт нарушения, возможно применение санкции согласно трудовому праву (выговор, блокирование доступа в Интернет, увольнение и т. д.).

Перед удалением данных, полученных путем нарушения правил, сотрудника информируют, и если его возможно оправдать, ему дается возможность перенести эти данные (например, личные электронные письма) на личный носитель информации.

5. Управление электронной почтой при отсутствии/уходе сотрудника

5.1 Ожидаемое отсутствие

При отсутствии более одного дня следует активировать в программе Outlook функцию «Автоответы (нет на работе)». В сообщении об отсутствии следует отметить, кто замещает вас по срочным делам (с указанием контактных данных), и перенаправляются ли письма автоматически. Автоматическое перенаправление писем заместителю следует применять только в исключительных случаях.

Если сотрудник по ошибке забыл включить функцию автоответов, следуйте инструкциям в пункте 6.

5.2 Непредвиденное отсутствие

При непредвиденном отсутствии (например, из-за болезни, несчастного случая) сотрудник обязан как можно быстрее настроить автоматическое перенаправление входящих писем. Это можно сделать, например, через надежный портал интернет-доступа к программе Outlook (<http://service.afg.ch>). Сотрудник также может назначить заместителя, который имеет право просматривать входящие служебные письма и при необходимости обрабатывать их. Если сотрудник не способен позаботиться о перенаправлении писем, следуйте инструкциям согласно пункту 6.

5.3 Непредвиденное продолжительное отсутствие

Если после непредвиденного отсутствия не планируется возвращение сотрудника на работу, или отсутствие продолжается очень долго (более 4 недель), в соответствии с пунктом 6 могут быть предприняты (дальнейшие) проверки.

5.4 Уход сотрудника

Увольняющийся сотрудник обязан передать все служебные документы. Перед уходом он обязан очистить жесткие диски и почту. Все активные дела, такие как электронные письма и т. п. или прочую необходимую и нужную AFG информацию следует передать другим сотрудникам.

Увольняющийся сотрудник имеет право удалить личные электронные письма и другие личные документы или сохранить их на личном носителе данных.

Не позднее последнего рабочего дня учетная запись пользователя (включая электронную почту) блокируется. Если после блокировки требуется просмотр учетной записи электронной почты или пользовательской папки, применяется право на инспекцию согласно пункту 6. Лицам, отправляющим письма на заблокированный электронный адрес, автоматически посылается информация о том, что данный адрес неактивен. По согласованию с руководителем в исключительных случаях можно активировать функцию «Автоответы (нет на работе)» и указать другой адрес электронной почты AFG. Необходимо следить за тем, чтобы из письма не было понятно, по каким причинам были прекращены трудовые отношения.

Через 30 дней после последнего рабочего дня, однако не ранее истечения увольнительного срока учетная запись пользователя удаляется.

6. Инспекция учетной записи сотрудника

Если, несмотря на меры, принятые согласно пункту 5.1, или в случае непредвиденного отсутствия требуется инспекция электронной почты сотрудника, сначала следует связаться с этим сотрудником и получить его согласие на проверку. Если сотрудник не дает согласия на инспекцию или недоступен, руководитель должен написать заявку в ответственный отдел кадров (см. приложение). Разрешение выдается только в том случае, если AFG имеет преобладающий интерес (например, неотложные, служебные дела), возврат сотрудника не ожидается, и были приняты все возможные меры, чтобы избежать инспекции. Автоматическое перенаправление всех электронных писем разрешается только в исключительных случаях.

Если на заявку дается положительный ответ, отправляется соответствующее сообщение в отдел информационных технологий, который восстанавливает пароль. Инспекцию учетной записи осуществляют руководитель и сотрудник отдела кадров (принцип «четырёх глаз»). Отсутствующего сотрудника информируют об этом не позднее дня его возвращения на рабочее место.

Продолжительность и содержание инспекции должны быть ограничены указанными в бланке заявления данными. Разрешается просматривать только служебные электронные письма. Запрещается открывать, просматривать, перемещать, копировать, пересылать и/или удалять личные письма (см. пункт 3). Руководитель пересылает необходимые электронные письма на свой адрес самостоятельно. Кроме того, следует активировать функцию «Автоответы (нет на месте)», указав, к кому обращаться по срочным вопросам.

Эти предписания действуют аналогичным образом после ухода сотрудника и для проверки пользовательских папок.

7. Подозрение в преступном поведении

Если при анализе зарегистрированных данных или по другим указаниям установлено или предполагается совершение преступления, необходимо защитить соответствующие протоколы. Компания AFG оставляет за собой право заявить о преступлении, совершенном подозреваемым лицом. Если необходима инспекция личной электронной почты, данных и т. д., проводить ее следует только получив предварительное согласие подозреваемого сотрудника. Если получить предварительное согласие невозможно, или подозреваемый не дает своего согласия, то инспекцию личных данных следует поручить компетентному правоохранительному

органу. Если преобладающий интерес и конкретные подозрения оправдывают это, то в качестве исключения AFG может провести инспекцию самостоятельно. Инспекция осуществляется согласно пункту 6.

AFG обязуется хранить результат расследования в тайне от третьих лиц, особенно от других сотрудников.

8. Информация

Справочную информацию относительно данной инструкции можно получить у главы юридического отдела предприятия.

9. Вступление в силу

Данная инструкция вступает в силу немедленно.

Арбон, 29 августа 2013 г.

AFG Arbonia-Forster-Holding AG

Daniel Frutig
исполнительный директор

Andrea Wickart
начальник контрольно-правового отдела
Генеральный секретарь

Приложение: Бланк заявления на получение права инспекции учетной записи сотрудника

Сотрудник, подлежащий проверке	
Фамилия, имя:	Компания:
Должность:	
Предмет инспекции:	
<input type="checkbox"/> электронная почта	<input type="checkbox"/> данные
Причина инспекции	
<input type="checkbox"/> запланированное отсутствие	ожидаемая дата возвращения:
<input type="checkbox"/> непредвиденное отсутствие	
<input type="checkbox"/> сотрудник уволился	Дата увольнения:
<input type="checkbox"/> подозрение в преступном поведении	Конкретные причины подозрения:
Инспекция крайне необходима, т. к.	
Объем инспекции (как можно более подробно)	
Крайне необходимы электронные письма или данные по следующим темам:	Необходимо найти электронные письма или данные, созданные в следующий период времени:
Согласие сотрудника, подлежащего инспекции	
<input type="checkbox"/> Да, была попытка получить предварительное согласие данного сотрудника, результат следующий:	<input type="checkbox"/> Нет, попытки получить предварительное согласие данного сотрудника не было, т. к.:
Альтернативы	
Чтобы избежать инспекции, были предприняты следующие действия:	
<input type="checkbox"/> Проведен поиск необходимых данных в общей папке (G:/общая учетная запись электронной почты).	<input type="checkbox"/> Сделан запрос необходимых данных/электронных писем у других членов команды отсутствующего.
<input type="checkbox"/> Прочее:	
Место/дата	Подпись

--	--