

Política sobre

- el uso y seguimiento del control del tráfico de Internet y del correo electrónico y las llamadas telefónicas; así como**
- la consulta de la cuenta de usuario de un empleado**

4 de diciembre de 2014

Índice

Preámbulo	3
1. Uso de servicios de internet y de telefonía.....	3
2. Control de servicios de internet y de telefonía.....	3
2.1 Registros	3
2.2 Prohibición de programas espía.....	3
2.3 Evaluación de los registros.....	3
2.4 Control como garantía de seguridad y funcionamiento del sistema informático de la empresa	4
2.5 Duración de la conservación	4
3. Distinción entre correos electrónicos privados y comerciales.....	4
4. Sanciones por uso indebido	4
5. Gestión del correo electrónico en caso de ausencias/renuncia de empleados	5
5.1 Ausencia prevista.....	5
5.2 Ausencia imprevista.....	5
5.3 Ausencia imprevista de larga duración	5
5.4 Renuncia de un empleado	5
5.5 Excepciones de las secciones 5.1 a 5.4.....	5
6. Consulta de la cuenta de usuario de los empleados	6
7. Sospecha de un comportamiento delictivo	6
8. El uso de nubes.....	6
9. Discrepancias	7
10. Información	7
11. Entrada en vigor.....	7
Anexo 1: Formulario de solicitud para el derecho a consulta de la cuenta de usuario de un empleado	8
Anexo 2: Excepciones de las secciones 5.1 a 5.4 de la Política sobre el seguimiento y uso de Internet, correo electrónico y teléfono	9

Preámbulo

Esta Política establece si los empleados de las empresas del grupo AFG Arbonia-Forster-Holding AG (en lo sucesivo, "AFG") pueden utilizar los servicios telefónicos y de Internet y de qué manera. Asimismo, esta Política tiene como objetivo proteger a los empleados y AFG a la hora de controlar estos servicios y consultar una cuenta de usuario. Debe respetarse la normativa local que establezca disposiciones más estrictas o que se utilice para la aplicación de la Política.

1. Uso de servicios de internet y de telefonía

Si los servicios de Internet (Internet/correo electrónico) y los servicios telefónicos están disponibles para los empleados, estos están destinados a fines comerciales y pensados para permitirles trabajar mejor o de manera más eficiente o profesional.

El director general de la unidad de negocios¹ decide si el uso se extiende exclusivamente a los intereses comerciales.

No deben visitarse páginas web con contenido delictivo, pornográfico o racista. También está prohibida la participación en dichas actividades (por ejemplo, mediante el intercambio de ideas a través de chats, correos electrónicos, etc.). Pueden utilizarse filtros automáticos para bloquear el contenido de determinadas categorías. Se trata de páginas con el siguiente contenido: pornografía, actividades delictivas, contenido extremista, chat, drogas.

Por razones de seguridad, todos los correos electrónicos y el acceso a Internet, incluidas las descargas, se comprueban automáticamente en busca de virus y contenido peligroso y se bloquean en caso necesario. Esto también se aplica a las conexiones cifradas a Internet (por ejemplo, banca online). No obstante, los correos electrónicos de remitentes desconocidos o aquellos que indiquen un virus en el asunto deben eliminarse de inmediato sin ser leídos. En ningún caso deben abrirse archivos adjuntos de correo electrónico de remitentes desconocidos.

2. Control de servicios de internet y de telefonía

2.1 Registros

El departamento informático registra las actividades de Internet. Se registran las llamadas telefónicas entrantes y salientes. El registro se define como la grabación continua de datos marginales "quién", "qué", "cuándo" y tiene lugar en AFG en los siguientes puntos:

- Internet (páginas web visitadas, usuarios, fecha, hora)
- Correo electrónico (remitente, destinatario, fecha, hora, línea de asunto)
- Inicio de sesión en el sistema (usuario, fecha, hora)
- Teléfono (números de teléfono de todos los participantes, hora, fecha, duración)

2.2 Prohibición de programas espía

No pueden utilizarse programas espía (llamados spyware). Los programas espía son aquellos programas que permiten que los empleados sean controlados sin su conocimiento.

2.3 Evaluación de los registros

Los registros se evalúan a diferentes niveles.

¹ En el caso de los empleados de AFG Management AG, es el CEO quien toma la decisión.

Evaluación anónima: se utiliza para generar estadísticas, como la visualización estructurada del uso medio de Internet, las páginas web visitadas con más frecuencia, etc. El número de personas analizadas debe mantenerse lo suficientemente grande para que no sea posible sacar conclusiones sobre empleados concretos (por ejemplo, todos los empleados de AFG Management AG).

Evaluación personal: solo se permite una evaluación personal si la evaluación anónima ha identificado un mal uso o si existe cualquier otra sospecha de mal uso. Cualquier incumplimiento de los términos de uso de acuerdo con la sección 1 de esta Política u otras obligaciones contractuales se considera un uso indebido.

La evaluación personal se lleva a cabo a petición del supervisor y la realiza el departamento de RR. HH. responsable de manera conjunta con el departamento informático y, si existe, el delegado de protección de datos. Si no se fundamenta una sospecha de uso indebido, las evaluaciones personales se detendrán de inmediato y se destruirán los datos recopilados.

2.4 Control como garantía de seguridad y funcionamiento del sistema informático de la empresa

Si se manifiesta un fallo en el sistema informático a pesar de las medidas de protección técnicas, pueden utilizarse los registros para encontrar la causa. Si la causa del fallo es un uso indebido, el empleado identificado puede ser sancionado de conformidad con la sección 4 de la presente Política.

2.5 Duración de la conservación

Los registros de las actividades de Internet se conservan durante cuatro semanas con el fin de preservar las pruebas, a menos que las sanciones o los procesos penales requieran una conservación más prolongada. La conservación de los registros telefónicos se basa en la normativa local aplicable en materia de telecomunicaciones.

3. Distinción entre correos electrónicos privados y comerciales

La cuenta de correo electrónico se utiliza principalmente para fines empresariales. Las comunicaciones privadas deben reducirse al mínimo. AFG no consulta ni procesa los correos electrónicos marcados como privados. Si no hay distinción entre correos electrónicos privados y comerciales y la naturaleza privada de un correo electrónico no puede identificarse ni asumirse de otra manera por los elementos de dirección, AFG asumirá que el correo electrónico es comercial. Si hay dudas respecto a la naturaleza de un correo electrónico, deberá aclararse con el empleado.

Además de la copia de seguridad del sistema, los correos electrónicos comerciales pueden guardarse fuera del buzón personal si es necesario.

Cuando se detecta que un correo electrónico es de carácter privado, es posible que AFG no tome nota de su contenido. Esto se aplica incluso si se sospecha que se ha cometido un delito penal por correo electrónico o que hay otro caso de uso indebido de conformidad con la sección 1 de la presente Política.

4. Sanciones por uso indebido

Si se han cumplido los requisitos previos y las normas de control y se ha constatado que ha habido un uso indebido, pueden imponerse sanciones en virtud del Derecho laboral (amonestación, bloqueo de acceso a Internet, rescisión, etc.).

Se informará al empleado afectado antes de la eliminación de los archivos que se hayan utilizado de modo indebido y, en caso de justificación, se le dará la oportunidad de almacenar los archivos en cuestión (por ejemplo, correos electrónicos privados) en un soporte de datos privado.

5. Gestión del correo electrónico en caso de ausencias/renuncia de empleados

5.1 Ausencia prevista

En caso de ausencias de un día o más, en Outlook debe estar activado el mensaje de fuera de la oficina. En la notificación de ausencia, debe tenerse en cuenta quién es el sustituto para asuntos urgentes (incluidos los datos de contacto) y si los correos electrónicos entrantes se reenvían automáticamente o no. El reenvío automático de todos los correos electrónicos al sustituto solo puede realizarse en casos excepcionales.

Si un empleado ha olvidado por error activar el mensaje de fuera de la oficina, proceda de conformidad con la sección 6.

5.2 Ausencia imprevista

En caso de ausencia imprevista (por ejemplo, enfermedad, accidente), el empleado se asegura lo antes posible de que se reenvíen los correos electrónicos entrantes urgentes. Esto puede hacerse, por ejemplo, utilizando el portal de acceso seguro correspondiente. El empleado también puede designar a un sustituto que esté autorizado para ver los correos electrónicos comerciales entrantes y, si es necesario, procesarlos. Si el empleado no puede reenviar los correos electrónicos, proceda de conformidad con la sección 6.

5.3 Ausencia imprevista de larga duración

Si, en caso de una ausencia imprevista, no se puede prever la vuelta al trabajo o si la ausencia es muy larga (más de 4 semanas), pueden realizarse (más) consultas de conformidad con la sección 6.

5.4 Renuncia de un empleado

El empleado saliente es responsable de la entrega de todos los documentos comerciales. Debe limpiar los discos y la bandeja de entrada antes de su renuncia. Deben reenviarse todas las operaciones pendientes, como correos electrónicos, etc., u otra información necesaria o útil para AFG. El empleado saliente también debe configurar el mensaje de fuera de la oficina, que le informa que la dirección de correo electrónico ya no es válida e contiene los datos de contacto del sucesor.

El empleado saliente tiene la opción de borrar correos electrónicos privados y otros documentos privados o guardarlos en un soporte de datos privado.

La cuenta de usuario (incluida la cuenta de correo electrónico) se bloqueará a más tardar el último día laboral efectivo. Si es necesario consultar la cuenta de correo electrónico o una carpeta de usuario después de que se haya bloqueado, el derecho de consulta se basa con arreglo a la sección 6 Si el empleado saliente no ha configurado el mensaje de fuera de la oficina, debe procederse de conformidad con la sección 6 y activarse el mensaje de fuera de la oficina. Debe asegurarse de que no puedan sacarse conclusiones sobre el tipo de cese de la relación laboral.

La cuenta de usuario se borrará a más tardar 30 días después del último día laboral efectivo. En casos excepcionales, la cuenta de usuario se borrará a más tardar 90 días después del último día laboral efectivo.

5.5 Excepciones de las secciones 5.1 a 5.4

Las excepciones permitidas de las secciones 5.1 a 5.4 se establecen en el Anexo 2.

6. Consulta de la cuenta de usuario de los empleados

Si es necesario consultar la cuenta de correo electrónico de un empleado a pesar de las disposiciones de la sección 5, primero es necesario ponerse en contacto con el empleado en cuestión y obtener su consentimiento para la consulta. Si este último se niega a la consulta o no puede ser localizado, el supervisor debe enviar una solicitud por escrito al departamento de RR. HH. responsable (véase el Anexo). La autorización solo se concede si AFG tiene un interés preponderante (por ejemplo, razones operativas urgentes), no se puede esperar a la vuelta del empleado y se han adoptado todas las medidas para evitar la consulta. El reenvío automático de todos los correos electrónicos solo está permitido en casos excepcionales.

Si se autoriza la solicitud, se envía un mensaje al departamento informático para permitir el acceso a la cuenta de usuario (restableciendo la contraseña o a partir de un enlace). El supervisor y un empleado del departamento de RR. HH. realizan la consulta (principio de solución entre dos). El empleado ausente será informado al respecto a más tardar el día que vuelva al trabajo.

La consulta debe limitarse en tiempo y contenido a la información proporcionada en el formulario de solicitud. Solo deben leerse los correos electrónicos comerciales. Los correos electrónicos reconocidos como privados no deben abrirse, verse, moverse, copiarse, reenviarse o borrarse (véase también la sección 3). El supervisor se reenvía a sí mismo los correos electrónicos necesarios. Además, debe activarse el mensaje de fuera de la oficina con la información para poder contactar en caso de asuntos urgentes.

Estas disposiciones se aplican de la misma manera después de que un empleado abandone la empresa y para la consulta de la carpeta de usuario.

7. Sospecha de un comportamiento delictivo

Si se determina o sospecha un delito a partir de la evaluación de los registros u otras indicaciones, se guardan los registros correspondientes. AFG se reserva el derecho a presentar una querrela contra la persona en cuestión. Si es necesario consultar correos electrónicos privados, datos, etc., solo podrá hacer con el consentimiento previo del empleado bajo sospecha. Si no es posible obtenerlo por adelantado o si se deniega el consentimiento, normalmente deberá remitirse el asunto a la autoridad competente para que se haga cumplir la ley. Como excepción, AFG puede consultarlo por sí sola si está justificado por un interés preponderante y sospechas específicas. La consulta se fundamenta en la sección 6 anterior.

AFG se compromete a tratar los resultados de las investigaciones como confidenciales frente a terceros, en particular frente a otros empleados.

8. El uso de nubes

Las nubes son infraestructuras informáticas virtuales para almacenar información en Internet (por ejemplo, Dropbox). El uso de nubes puede tener grandes ventajas, ya que es posible, por ejemplo, acceder a los datos almacenados en la nube desde casa o mientras viaja. Sin embargo, al mismo tiempo, las nubes también albergan importantes riesgos de seguridad. Por esta razón, el uso de una nube solo está permitido si ha sido autorizado por el director general de la unidad de negocios² después de obtener una recomendación por parte del departamento informático responsable.

² El CEO es responsable de los empleados de AFG Management AG.

9. Discrepancias

Solo se permiten discrepancias de las secciones mencionadas anteriormente tras consultar con el Head of Legal & Compliance.

10. Información

El Head of Legal & Compliance proporciona información relacionada con las presentes Disposiciones.

11. Entrada en vigor

Esta Política entrará en vigor de inmediato y sustituirá la Política sobre el seguimiento y uso de Internet, correo electrónico y teléfono del 29 de agosto de 2013.

Arbon, 4 de diciembre de 2014

AFG Arbonia-Forster-Holding AG

William J. Christensen
Chief Executive Officer

Andrea Wickart
Head of Legal & Compliance
Secretaria general

Anexo 1: Formulario de solicitud para el derecho a consulta de la cuenta de usuario de un empleado

Empleado afectado	
Nombre:	Empresa:
Función:	
Objeto de la consulta	
<input type="checkbox"/> Correos electrónicos	<input type="checkbox"/> Archivos
Motivo de la consulta	
<input type="checkbox"/> Ausencia prevista	Vuelta prevista para el día:
<input type="checkbox"/> Ausencia imprevista	
<input type="checkbox"/> El empleado ya ha renunciado	Renuncia el día:
<input type="checkbox"/> Sospecha de un comportamiento delictivo	Motivos específicos de sospecha:
Se necesita una consulta urgente porque	
Alcance de la consulta (lo más detallado posible)	
Se necesitan con urgencia correos electrónicos o archivos sobre los siguientes temas:	El objetivo es buscar correos electrónicos o archivos en el siguiente período:
Puesta en contacto con el empleado afectado	
<input type="checkbox"/> Sí, se ha intentado obtener el consentimiento previo del empleado afectado con el siguiente resultado:	<input type="checkbox"/> No, no se ha intentado obtener el consentimiento previo del empleado afectado porque:
Alternativas	
Se ha hecho lo siguiente para evitar la consulta:	
<input type="checkbox"/> Se han buscado los archivos necesarios en la carpeta compartida (unidad G:/ de cuenta de correo electrónico compartida).	<input type="checkbox"/> Se les ha pedido los archivos/correos electrónicos requeridos a otros miembros del equipo de la persona ausente.
<input type="checkbox"/> Otros:	
Lugar/fecha	Firma

Anexo 2: Excepciones de las secciones 5.1 a 5.4 de la Política sobre el seguimiento y uso de Internet, correo electrónico y teléfono

Por razones operativas y técnicas, las siguientes excepciones de las secciones 5.1 a 5.4 se aplican a la Tecnología de construcción:

Creación de mensaje de fuera de la oficina

En principio, no se crea un mensaje de fuera de la oficina dentro de la Tecnología de construcción. En el caso de ausencias previstas o imprevistas y tras la renuncia, se indica a los empleados afectados a que:

- (a) designen a un sustituto que esté autorizado para ver los correos electrónicos comerciales entrantes y, si es necesario, procesarlos; o
- (b) configuren el reenvío automático de todos los correos electrónicos entrantes.

La designación del sustituto o la configuración del reenvío automático solo puede realizarla el propio empleado.

Eliminación de la cuenta de usuario tras la renuncia de un empleado

Por lo general, la cuenta de usuario se borrará 30 días después del último día laboral efectivo, pero como muy pronto cuando haya expirado el período de notificación. En casos excepcionales, la eliminación puede producirse en un momento posterior, pero a más tardar cuando se haya cumplido el propósito operativo.