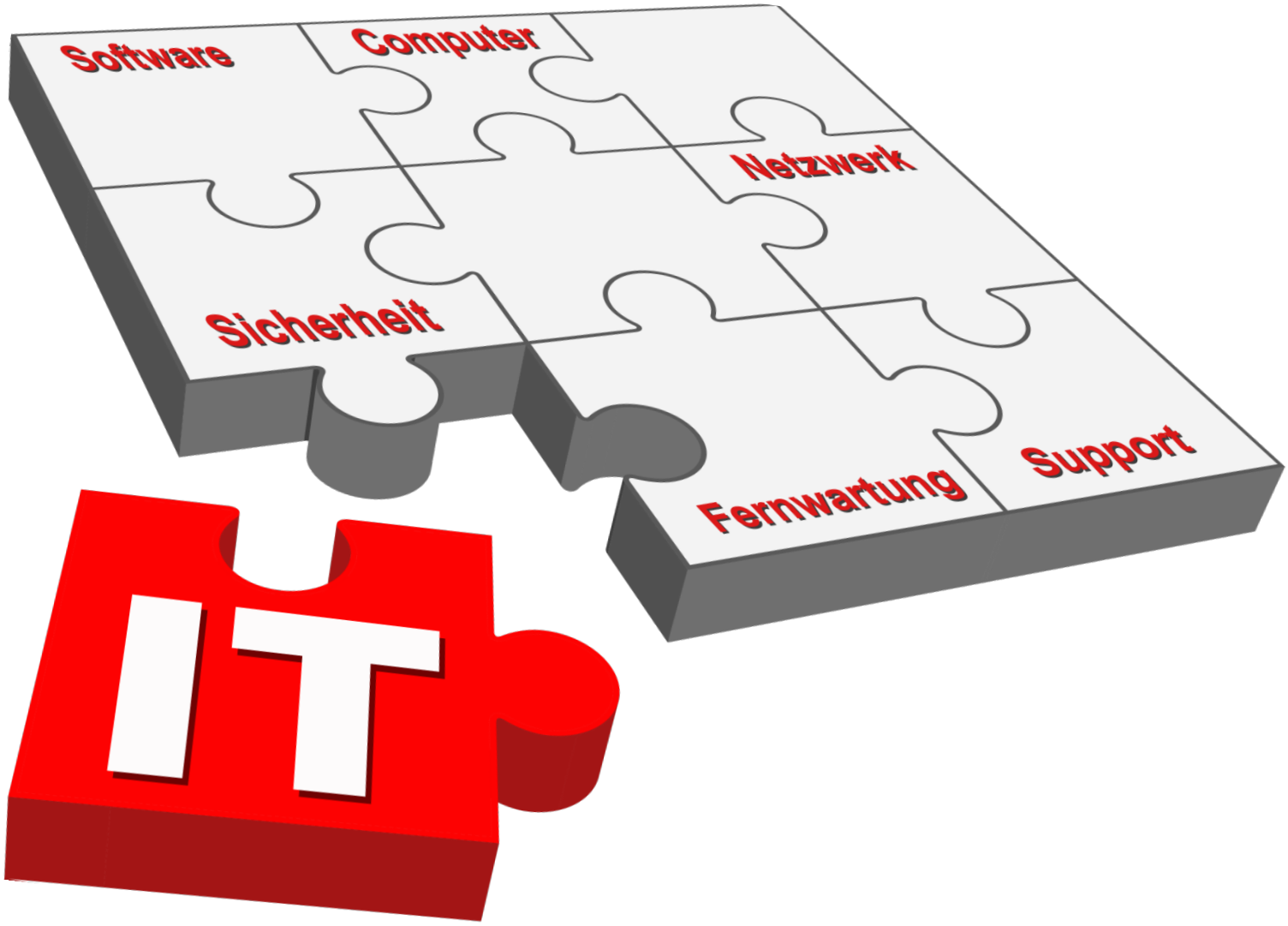
HYDAC INTERNATIONAL

Directiva de seguridad TI para proveedores de servicios externos

Última modificación:
febrero de 2016



1. Utilidad y ámbito de validez

Esta directiva de seguridad es de aplicación obligatoria para todos los proveedores de servicios externos que trabajan para una empresa relacionada con Hydac. Estas directrices deben entenderse como requisito mínimo para una prestación de servicios dentro de la empresa Hydac.

Si el proveedor de servicios externo no está en condiciones de cumplir estos requisitos mínimos, HYDAC no colaborará con este proveedor de servicios externo.

Se aplicará siempre la última versión autorizada y cargada en http://hyd.ac/itsicherheit de esta directiva de seguridad TI para proveedores de servicios externos.

2. Responsabilidades

El proveedor de servicios externo debe garantizar que la prestación del servicio se realice según la presente directiva.

- El proveedor de servicios externo contratado debe garantizar en todo momento que sus acciones y las acciones de sus empleados no comprometan la disponibilidad, integridad o confidencialidad de los sistemas TI de las empresas relacionadas con HYDAC.
- Deben cumplirse todas las disposiciones relativas a los derechos de autor y las patentes, así como acuerdos de licencia.
- Los datos de acceso facilitados no deben transmitirse a terceros.

3. Acceso a instalaciones y plantas de producción

El proveedor de servicios externo debe indicarle a sus empleados que deben darse de alta en la empresa relacionada con HYDAC a través de su persona de contacto. El proveedor de servicios externo también avisará a sus empleados de que si no disponen de un carné de visitante personalizado, se les entregará un carné de visitante y el documento "Indicaciones de seguridad para visitantes" y de que deben llevar este carné de forma visible en todo momento.

4. Uso de sistemas e infraestructuras TI de HYDAC

Normas y derechos de uso

El software y hardware que se utilice dentro de la infraestructura de HYDAC no debe comprometer en ningún momento la seguridad ni el rendimiento de dicha infraestructura. Por ello, el proveedor de servicios externo solo debe utilizar productos y dispositivos autorizados por el departamento TI central.

Uso de internet e infraestructuras de comunicación

El departamento TI central protocoliza todos los accesos por motivos de diagnóstico y seguridad.

Si se ha facilitado el acceso a recursos de internet o cuentas de correo electrónico de HYDAC, el proveedor de servicios externo debe advertir a sus empleados de que solo se permite el uso de internet y el correo electrónico con motivos laborales.

Los sistemas TI del entorno de producción no deben tener acceso a internet.

El uso de "soluciones en la nube" está prohibido.

Gestión de software y hardware

El proveedor de servicios externo solo debe facilitar, instalar o montar componentes TI si dichos componentes han sido revisados y aprobados por el departamento TI central antes de su conexión a la red de HYDAC.

Para la aprobación de elementos de hardware o software debe presentarse una serie de documentos por escrito. Estos documentos deben incluir al menos los siguientes puntos:

- Configuración de los componentes y funciones de red
- Función del software
- Interfaces
- Derechos requeridos
- Datos de acceso

Los componentes TI empleados por el proveedor de servicios externo deben ser compatibles con las soluciones TI elegidas por HYDAC. El proveedor de servicios externo debe consultar dichas soluciones en el departamento TI central.

Cualquier modificación en el hardware o software de un terminal (p. ej. montaje de discos duros, ampliación de la memoria, tarjetas WLAN) deben coordinarse con el departamento TI central. Los componentes TI también se deben desechar en colaboración con el departamento TI central.

A la hora de emplear medios de almacenamiento externo (p. ej. lápices de memoria USB, discos duros externos, dispositivos USB), debe garantizarse que solo se usan medios autorizados por HYDAC.

De forma adicional, los sistemas TI de producción deben cumplir los requisitos especificados en el documento *Requisitos TI generales mínimos en el entorno de producción HYDAC* que se puede consultar en http://hyd.ac/itstandardproduction.

Red

La infraestructura de red HYDAC solo debe ser manipulada por los correspondientes servicios autorizados. Queda prohibido cualquier cambio no autorizado por el departamento TI central.

El acceso ilimitado a la red queda reservado a los terminales propios de HYDAC y los terminales autorizados que están bajo la administración del departamento TI central.

El uso y la aplicación de componentes WLAN solo están permitidos previa consulta al departamento TI central.

5. Requisitos de seguridad mínimos

El proveedor de servicios externo debe garantizar que en el hardware facilitado y empleado se haya instalado la versión más reciente de un sistema antivirus y una base de datos de firma de virus.

Dicho sistema de protección debe incluir los siguientes componentes:

- OnAccessScanner
- OnDemandScanner
- Escaneo de correos electrónicos
- Host Intrusion Prevention System
- Cortafuegos local

Es obligatorio realizar un escaneo completo del sistema al menos una vez a la semana.

Deben instalarse las últimas actualizaciones del sistema operativo y el software empleado y debe comprobarse sus estado de actualización como mínimo una vez cada tres meses.

Además, el proveedor de servicios externo debe garantizar que sus empleados reciban una formación relativa a la seguridad TI. Si la prestación del servicio requiere la recopilación de datos de carácter personal o si no se puede descartar el acceso a datos de carácter personal, entonces el proveedor de servicios externo debe asegurarse de que sus empleados hayan sido instruidos según el art. 5 de la Ley alemana de protección de datos y de que actúen de acuerdo a la ley.

La transmisión de datos de empresas relacionadas con HYDAC a terceros está prohibida. Siempre y cuando no exista una autorización excepcional.

Todo el tráfico de correo electrónico entre HYDAC y el proveedor de servicios externo debe tratarse con la máxima confidencialidad.

Está prohibido guardar datos de HYDAC sin codificar en soportes móviles de datos (p. ej. lápices de memoria USB). Cualquier excepción requiere una autorización especial por parte del departamento TI central.

Todos los datos generados en el marco de la prestación del servicio para empresas relacionadas con HYDAC pertenecen a la sociedad de HYDAC que ha encargado el servicio.
Una vez finalizado el trabajo, deben devolverse todos los datos a la sociedad de HYDAC que ha encargado
el servicio, sin conservar copias, extractos o cualquier otra reproducción total o parcial.

6. Comportamiento en caso de problemas técnicos

El proveedor de servicios externo debe advertir a sus empleados de que en caso de problemas técnicos o un incidente de seguridad TI durante el funcionamiento, debe informarse inmediatamente a la persona de contacto de HYDAC.

7. Regulación de las cuentas de usuario facilitadas

Los derechos de acceso facilitados y el uso de datos de carácter personal o de cualquier otro tipo de datos de la empresa sirven exclusivamente para cumplir el objeto del contrato.

El proveedor de servicios externo debe garantizar que todos los empleados puedan iniciar sesión con su cuenta asignada de usuario. La cuenta de usuario y la contraseña no deben

transmitirse a terceros. La contraseña debe cumplir con los requisitos de las directivas de HYDAC.

Antes de la finalización del contrato de prestación de servicios el proveedor de servicios externo debe asegurarse de que todos los carnés y soportes de datos entregados a sus empleados se devuelvan a HYDAC. Todas las cuentas de usuario de empleados del proveedor de servicios externo que ya no se van a usar deben comunicarse inmediatamente al departamento TI central para que procedan a su desactivación.

8. Acceso/mantenimiento remoto

El acceso local a la red HYDAC siempre debe anteponerse a un acceso remoto. Un acceso remoto solo es posible después de consultar el caso con el departamento TI central y cumpliendo las siguientes regulaciones:

- El acceso remoto para el mantenimiento remoto solo se facilita a través del gateway HYDAC SSL, cualquier otra opción no es compatible.
- El proveedor de servicios externo debe asegurarse que la red propia de sus empleados no permita un acceso sin supervisión de terceros a la red HYDAC.
- Solo se permite el uso de conexiones y software autorizados por el departamento TI central para el mantenimiento remoto.
- Ningún sistema TI debe establecer una conexión VPN por iniciativa propia.
- El proveedor de servicios externo está obligado a comprobar la funcionalidad del acceso remoto al menos una vez cada tres meses.

9. Prestación de servicio

Software

Si el proveedor de servicios externo realiza servicios en el marco del desarrollo de software, se aplicarán las siguientes regulaciones en el siguiente orden:

- Condiciones generales de compra y
- Condiciones especiales de compra para productos de software y/o
- Condiciones especiales de compra para máquinas e instalaciones.

Debe garantizarse que el código fuente de los productos de software desarrollados esté accesible. Para ello, existen las siguientes posibilidades:

- Entrega del código fuente y el entorno de desarrollo.
- Depósito del código fuente y del entorno de desarrollo ante notario.

Hardware

El hardware debe diseñarse en colaboración con la persona de contacto de HYDAC y de acuerdo con las directivas internas.