IT-Sicherheitsrichtlinie - Externe Dienstleister

Februar 2018

1. Geltungsbereich und Zweck

Diese Sicherheitsrichtlinie ist verpflichtend für alle externen Dienstleister, die für ein Unternehmen des HYDAC-Firmenverbundes (Im Folgenden: HYDAC) tätig sind. Diese Vorgaben sind als Mindestanforderung für eine Dienstleistungserbringung innerhalb der HYDAC zu verstehen.

Soweit diese Mindestanforderungen durch den externen Dienstleister nicht erfüllt werden können, wird HYDAC nicht mit diesem externen Dienstleister zusammenarbeiten.

Es gilt die jeweils unter http://hyd.ac/itsicherheit hinterlegte letzte freigegebene Version dieser IT- Sicherheitsrichtlinie - Externe Dienstleister.

2. Verantwortlichkeiten

Der externe Dienstleister hat dafür zu sorgen, dass die Dienstleistungserbringung der hier vorliegenden Richtlinie folgt.

- Der beauftragte externe Dienstleister hat jederzeit sicher zu stellen, dass sein Handeln und das Handeln seiner Beschäftigten nicht die Verfügbarkeit, Integrität oder Vertraulichkeit der IT-Systeme und Daten der HYDAC beeinträchtigt.
- Urheberrechtliche und patentrechtliche Bestimmungen sowie Lizenzvereinbarungen sind einzuhalten.
- Die aktuellen Richtlinien und Normen zum Datenschutz sind einzuhalten.
- Die bereitgestellten Zugangsdaten dürfen nicht an Dritte weitergegeben werden.

3. Zugang zu Gebäuden und Produktionsstätten

Der externe Dienstleister muss seine Beschäftigten darauf hinweisen, dass diese sich bei ihrem Ansprechpartner in einem HYDAC verbundenen Unternehmen anzumelden haben. Der externe Dienstleister wird seine Beschäftigten ebenso darauf hinweisen, dass diesen, sollten sie keinen personalisierten Besucherausweis haben, ein Besucherausweis und das Formblatt „Sicherheitshinweise für Besucher übergeben wird und dass sie diesen Ausweis deutlich sichtbar tragen müssen.

4. Nutzung von HYDAC IT-Systemen und IT-Infrastrukturen

Nutzungsgrundlage und Nutzungsrechte

Innerhalb der HYDAC Infrastruktur eingesetzte Hard- und Software darf die Sicherheit und Leistungsfähigkeit der Infrastruktur nicht beeinträchtigen. Daher darf der externe Dienstleister nur vom Zentralbereich IT freigegebene Produkte und Geräte verwenden.

Nutzung von Internet und Kommunikationsinfrastruktur

Alle Zugriffe werden vom Zentralbereich IT zu Diagnose- und Sicherheitszwecken protokolliert.

Der externe Dienstleister hat seine Beschäftigten darauf hinzuweisen, dass wenn der Zugriff auf Internetressourcen oder HYDAC E-Mailaccounts bereitgestellt wurde, die Nutzung von Internet und E- Mail ausschließlich für geschäftliche Zwecke erlaubt ist.

IT-Systeme im Produktionsumfeld dürfen keinen Internetzugriff erhalten.

Die Verwendung von „Cloud-Lösungen“ ist untersagt.

Hard- und Softwaremanagement

Der externe Dienstleister darf nur IT-Komponenten bereitstellen, installieren oder verbauen, wenn diese vor ihrem Anschluss an das HYDAC-Netzwerk vom Zentralbereich IT überprüft und freigegeben worden sind.

Zur Freigabe der Hard- bzw. Software muss eine schriftliche Dokumentation vorliegen. Diese Dokumentation muss mindestens folgende Punkte beinhalten:

- Konfiguration der Netzwerkkomponenten und –Funktionen
- Funktion der Software
- Schnittstellen
- Benötigte Berechtigungen
- Zugangsdaten
- Information ob Ressource kritisch ist

Die vom externen Dienstleister eingesetzten IT-Komponenten müssen die von HYDAC gewählten IT-Sicherheitslösungen unterstützen. Der externe Dienstleister muss diese beim Zentralbereich IT anfordern.

Modifikationen an der Hardware oder Software eines Endgerätes (wie z.B. Einbau von Festplatten, Speichererweiterung, WLAN Karten) müssen mit dem Zentralbereich IT koordiniert werden. IT-Komponenten werden in Abstimmung mit dem Zentralbereich IT entsorgt.

Bei der Nutzung von externen Speichermedien (z.B. USB-Stick, externe Festplatte, USB-Geräte) ist darauf zu achten, dass lediglich von HYDAC freigegebene Medien genutzt werden dürfen.

Zusätzlich müssen für IT-Systeme in der Produktion die Anforderungen innerhalb des Dokuments *Generelle IT Mindestanforderungen im Umfeld der HYDAC Produktion* eingehalten werden, abrufbar unter http://hyd.ac/it-standard-production .

Netzwerk

Die HYDAC- Netzwerkinfrastruktur wird ausschließlich von den dafür autorisierten Stellen betrieben. Jegliche nicht vom Zentralbereich IT autorisierte Modifikation ist untersagt.

Ein uneingeschränkter Netzwerkzugriff ist nur für HYDAC eigene bzw. freigegebene und durch den Zentralbereich IT administrierte Endgeräte erlaubt.

Die Verwendung und der Betrieb von WLAN-Komponenten dürfen nur nach Rücksprache mit dem Zentralbereich IT erfolgen.

Der Zugriff auf nichtöffentliche Teile der HYDAC IT-Infrastruktur ist auf die Notwendigkeit der

durchzuführenden Arbeit zu beschränken. Ein Zugriff darüber hinaus darf nur nach Abstimmung mit dem Zentralbereich IT erfolgen.

5. Sicherheitstechnische Mindestanforderungen

Der externe Dienstleister muss sicherstellen, dass auf der von ihm verwendeten und bereitgestellten Hardware die aktuellste Version eines Virenschutzsystems mit einer aktualisierten Virensignatur-Datenbank installiert ist.

Dieses Schutzsystem muss folgende Komponenten umfassen:

- OnAccessScanner
- OnDemandScanner
- E-Mailscan
- Host Intrusion Prevention System
- Lokale Firewall

Ein mindestens wöchentlicher Komplettscan des Systems ist verpflichtend.

Die aktuellen Updates für Betriebssystem und verwendete Software müssen installiert und mindestens einmal pro Vierteljahr auf Aktualität geprüft werden.

Weiterhin muss der externe Dienstleister sicherstellen, dass seine Beschäftigten eine Unterweisung hinsichtlich IT-Sicherheit erhalten haben. Sollte zur Erbringung der Dienstleistung die Verarbeitung von personenbezogenen Daten notwendig sein bzw. wenn der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, muss der externe Dienstleister sicherstellen, dass seine Beschäftigten nach Art. 5, Art. 24, Art. 29, Art. 32, Art. 39 Abs.1 lit a DSGVO unterwiesen und verpflichtet sind.

Das Verarbeiten von personenbezogenen Daten ist durch einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO dokumentiert und geregelt.

Die Übertragung von Daten der HYDAC verbundener Unternehmen an Dritte ist nicht zulässig, sofern keine gesonderte Genehmigung vorliegt.

Sämtlicher E-Mail-Verkehr zwischen HYDAC und dem externen Dienstleister ist vertraulich zu behandeln.

Das Speichern von Daten der HYDAC in unverschlüsselter Form ist auf mobilen Datenträgern (z.B. USB-Sticks) unzulässig. Ausnahmen erfordern eine gesonderte Genehmigung durch den Zentralbereich IT.

Daten aller Art, die im Rahmen der Abarbeitung des Auftrags für HYDAC verbundene Unternehmen generiert werden, befinden sich im Eigentum der beauftragenden HYDAC-Gesellschaft.
Nach Abschluss der Arbeiten sind Daten aller Art an die beauftragende HYDAC-Gesellschaft zurückzugeben, wobei keine Kopien, Auszüge oder sonstige vollständige oder teilweise Reproduktionen einbehalten werden dürfen.

Das eigenständige Verschlüsseln von Daten durch den Dienstleister ist strengstens untersagt. Wird eine Verschlüsselung in Erwägung gezogen, so ist diese mit dem Zentralbereich IT abzustimmen und unterliegt den Firmenstandards.

6. Umgang mit technischen Störungen

Der externe Dienstleister hat seinen Beschäftigten darauf hinzuweisen, dass wenn während des Betriebs Störungen auftreten oder ein IT-Sicherheitsvorfall bekannt wird, umgehend der HYDAC Ansprechpartner informiert werden muss.

7. Regelung bereitgestellte Benutzerkonten

Die erteilten Zugriffsberechtigungen und die Verwendung personenbezogener oder anderer betrieblichen Daten dienen ausschließlich der Erfüllung des Vertragsgegenstandes.

Der externe Dienstleister hat dafür zu sorgen, dass sich jeder eingesetzten Beschäftigten mit der für ihn beantragten Benutzerkennung anmelden kann. Die Benutzerkennung und das Passwort dürfen nicht an Dritte weitergegeben werden. Das Passwort muss den HYDAC Richtlinien entsprechen.

Bei Beendigung des Dienstleistungsvertrages muss der externe Dienstleister veranlassen, dass alle Ausweise und ausgehändigten Datenträger durch seine Beschäftigten an HYDAC zurückgeben werden. Nicht mehr benötigte Benutzerkonten von Beschäftigten des externen Dienstleisters müssen dem Zentralbereich IT zwecks Deaktivierung unverzüglich gemeldet werden.

8. Fernwartung / Fernzugriff

Der lokale Zugriff auf das HYDAC Netzwerk ist einem Fernzugriff immer zu vorzuziehen. Ein Fernzugriff ist nur nach Rücksprache mit dem Zentralbereich IT und den nachfolgend aufgeführten Regelungen möglich.

- Der Remote Zugriff zur Fernwartung wird nur über das HYDAC SSL Gateway bereitgestellt, jegliche anderen Möglichkeiten werden nicht unterstützt.
- Der externe Dienstleister muss sicherstellen, dass das eigene Netzwerk seines Beschäftigten keinen unkontrollierten Zugriff Dritter auf das HYDAC Netzwerk ermöglicht.
- Es dürfen nur durch den Zentralbereich IT freigegebene Verbindungen bzw. Software zur Fernwartung genutzt werden.
- Kein IT-System darf eigenständig eine VPN-Verbindung aufbauen.
- Der externe Dienstleister ist verpflichtet, die Funktionalität des Fernzugriffs mindestens einmal pro Vierteljahr zu testen.

9. Leistungserbringung

Software

Werden vom externen Dienstleister Leistungen im Bereich der Softwareentwicklung erbracht, kommen folgende Regelungen in nachfolgender Reihenfolge zur Anwendung:

- Allgemeine Einkaufsbedingungen, und
- Besondere Einkaufsbedingungen für Softwareprodukte, und/oder.
- Besondere Einkaufsbedingungen für Maschinen und Anlagen.

Es ist sicherzustellen, dass für entwickelte Softwareprodukte der Quellcode zugänglich ist. Dazu bestehen folgende Möglichkeiten:

- Aushändigung des Quellcodes und der Entwicklungsumgebung.
- Hinterlegung des Quellcodes und der Entwicklungsumgebung bei einem Notar.

Hardware

Die Hardware ist in Absprache mit dem Ansprechpartner bei HYDAC den internen Richtlinien entsprechend auszulegen.

10. Umgang mit personenbezogenen Daten

Erfolgt eine Verarbeitung von personenbezogenen Daten im Auftrag, so bietet der Dienstleister

hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutzgrundverordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

HYDAC wird vor Auftragsbeginn mit dem Dienstleister einen Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 2 abschließen.