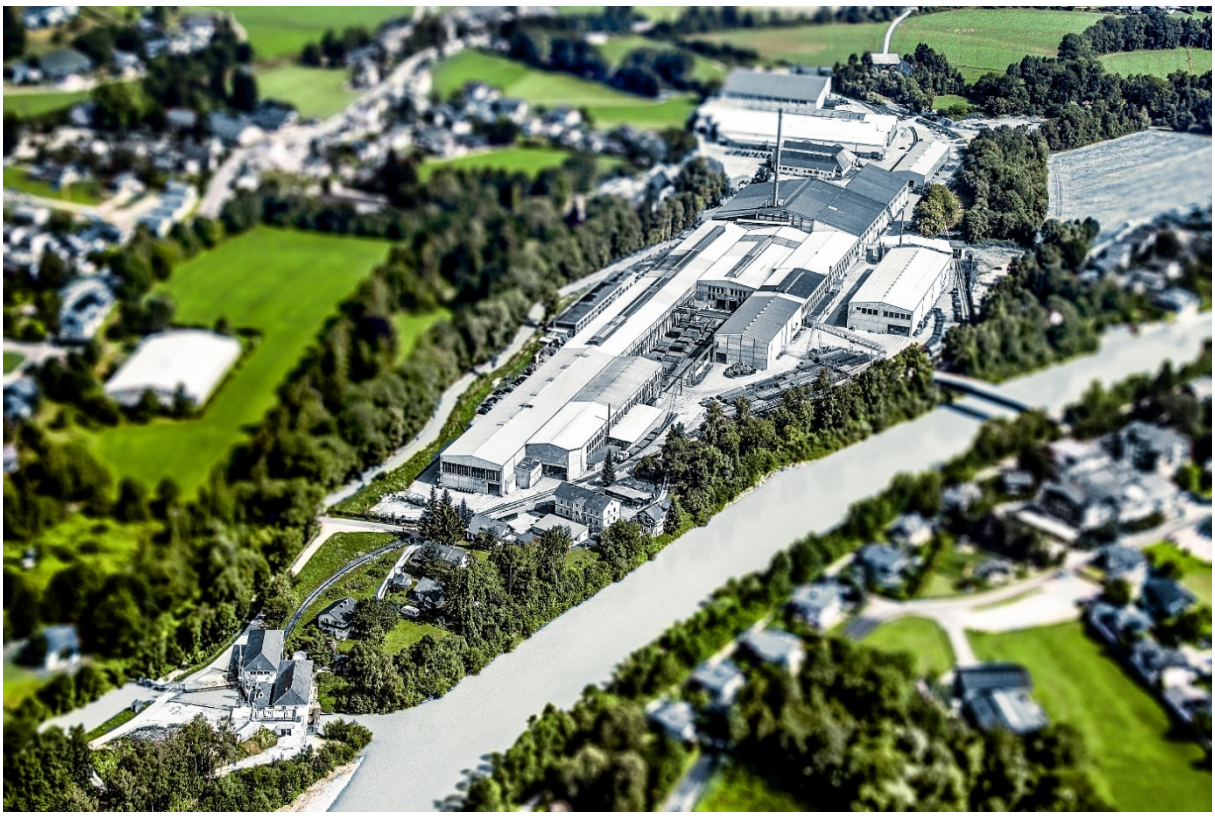
VERBINDLICHE IT- SICHERHEITSVORGABEN FÜR DIENSTLEISTER

der Stahlwerk Annahütte Max Aicher GmbH & Co. KG



Stahlwerk Annahütte Max Aicher GmbH & Co. KG
Max-Aicher-Allee 1+2
83404 Ainring/Hammerau
www.annahuette.com
stahlwerk@annahuette.com

Version 2.0 Stand März 2020

1. Inhaltsverzeichnis

2 Gegenstand 2

3 Geltungsbereich, Subunternehmer und Nachweise 2

4 Allgemeine Sicherheitsvorgaben 2

4.1 Virenschutz 2

4.2 Patch Management 2

4.3 Netzwerksicherheit 2

4.4 Physikalischer Zutritt 2

4.5 Zugangs- und Zugriffsrechte 3

4.6 Aufbewahrung und Speicherung von Kennwörtern 3

4.7 System Dienste und Benutzerkonten 3

4.8 Datenspeicherung und Mitnahme 3

4.9 Cloud-Dienste etc. 3

4.10 Vor Ort Tätigkeiten 4

5 Vorgaben Remote Einwahl 4

6 Umgang mit Administratorenrechten 4

7 Allgemeine Verpflichtungen 5

7.1 Meldepflicht, Zugangs- und Zugriffssperrung 5

7.2 Nutzung von Informationen des Auftraggebers 5

7.3 Datengeheimnis 6

7.4 Mitarbeiterqualifikation 6

2. Gegenstand

Die hiesigen IT-Sicherheitsvorgaben für Dienstleister beinhalten seitens der Stahlwerk Annahütte Max Aicher GmbH & Co. KG (auch kurz: „Auftraggeber“) verbindliche Mindestanforderungen an die IT-Sicherheit beim Auftragnehmer.
Diese IT-Sicherheitsvorgaben sind für den Zugang und Zugriff auf IT-Systeme, Dienste, Daten und Anwendungen in Netzwerken der Stahlwerk Annahütte durch den Auftragnehmer und dessen Subunternehmer verbindlich.
Im Einzelfall können vom Auftraggeber zusätzliche auftrags- oder systembezogene Sicherheitsvorgaben ergänzt werden.

3. Geltungsbereich, Subunternehmer und Nachweise

Der Auftragnehmer gewährleistet

- innerhalb seines Unternehmens und
- bei seinen Subunternehmen

die Einhaltung der hiesigen IT Sicherheitsvorgaben.
Ob und inwieweit der Auftragnehmer Sub-Unternehmer einsetzen darf, richtet sich nach den vertraglichen Vereinbarungen zwischen Auftraggeber und Auftragnehmer.
Auf Aufforderung des Auftraggebers weist der Auftragnehmer die Einhaltung der IT-Sicherheitsvorgaben und gegebenenfalls die Verpflichtung auch seiner Subunternehmer darauf nach.

4. Allgemeine Sicherheitsvorgaben

4.1 Virenschutz

Der Auftragnehmer muss sicherstellen, dass auf der von ihm und seiner Subunternehmen verwendeten und bereitgestellten Hardware (z. B. PCs, Server, Gateways) die aktuellste Version eines anerkannt sicheren Virenschutzsystems mit einer regelmäßig aktualisierten Virensignatur-Datenbank installiert ist.

4.2 Patch Management

Der Auftragnehmer und seine Subunternehmen müssen über einen definierten Patch-Management-Prozess sicherstellen, dass auf der von ihm verwendeten Hardware aktualisierten Sicherheits-Patches für die Betriebssystem-Software und Anwendungen installiert sind.

4.3 Netzwerksicherheit

Der Auftragnehmer und seine Subunternehmen müssen sicherzustellen, dass deren Netzwerk sowie die IT-Systeme jeweils ausreichend und nach dem aktuellen Stand der Technik vor Angriffen und Missbrauch geschützt sind, ebenso wie die Vertraulichkeit, Verfügbarkeit und Integrität der IT-Systeme, Dienste, Daten und Anwendungen gewährleistet ist.

4.4 Physikalischer Zutritt

Es ist zu gewährleisten, dass der physikalische Zutritt auf IT-Systeme und/oder Netzwerke des Auftragnehmers ausreichend und nach dem Stand der Technik geschützt sind.

4.5 Zugangs- und Zugriffsrechte

Ist für einen Auftragnehmer oder seine Subunternehmen ein Zugang/Zugriff zum Netzwerk eingerichtet hat der Auftragnehmer die nachfolgenden Regelungen zu beachten und dies etwaigen Subunternehmern aufzulegen:

(1) Jeder Mitarbeiter des Auftragnehmers muss sich mit seiner Benutzerkennung anmelden und sichere Kennwörter verwenden. Benutzerkennungen und Kennwörter dürfen nicht weitergegeben werden. Handelt es sich um ein gemeinsames Benutzerkonto, welches von mehreren Mitarbeitern verwendet wird, muss der Auftragnehmer sicherstellen, dass die Zugangsdaten nur dem dafür erforderlichen Personenkreis bekannt sind.
(2) Der Auftraggeber weist den Auftragnehmer darauf hin, dass Zugang und Zugriffe auf das Netzwerk protokolliert werden. Der Auftraggeber informiert hierüber seine Mitarbeiter und Subunternehmen.
(3) Der Auftragnehmer ist verpflichtet, den Auftraggeber umgehend zu informieren, wenn ein Zugang/Zugriff auf das Netzwerk nicht mehr erforderlich ist (z. B. Auftragsabschluss,
Mitarbeiterwechsel, Kündigung oder sonstige Beendigung des Auftrags).

4.6 Aufbewahrung und Speicherung von Kennwörtern

Sämtliche System – und Benutzerkennwörter des Auftraggebers darf der Auftragnehmer in seinen IT-Systemen und Netzwerken nur in einem anerkannt sicheren Passwortverwaltungsprogramm speichern. Der Auftragnehmer hat dabei sicherzustellen, dass nur berechtigte Personen auf diese Informationen zugreifen können.

4.7 System Dienste und Benutzerkonten

Benutzerkonten, die für die Einwahl (Fernwartung) und/oder dem Support bereitgestellt werden, darf der Auftragnehmer ausschließlich nur für diesen Zweck verwenden. Eine Nutzung als System-, Dienst- oder Administratorkonto ist nicht gestattet. Die Konten unterliegen der Passwort Policy und sind somit von einem regelmäßigen Passwortwechsel betroffen.

4.8 Datenspeicherung und Mitnahme

Ist eine Speicherung und/oder Mitnahme von Auftraggeber Daten, auf IT-Systemen oder Datenträger des Auftragnehmers oder eines Subunternehmers notwendig, so hat der Auftragnehmer sicherzustellen, dass betreffend dieser Daten ein ausreichender Zugangs- und Zugriffsschutz besteht. Dazu gehört in jedem Fall eine Verschlüsselung des betroffenen Datenträgers nach dem Stand der Technik (Bitlocker, etc.)

4.9 Cloud-Dienste etc.

Die Speicherung sowie der Transfer von Daten des Auftraggebers über Öffentliche Datenspeicher (Cloud Dienste) z.B. Microsoft OneDrive, DropBox etc. ist nur nach Rücksprache gestattet.

4.10 Vor Ort Tätigkeiten

Bei Tätigkeiten die vor Ort beim Auftraggeber stattfinden und mit IT-Equipment des Auftragnehmers durchgeführt werden, sind folgende Vorgaben zu beachten und einzuhalten.

(1) Vor Beginn der Arbeit, muss das Gerät durch die IT geprüft werden (Quickcheck Antivirenschutz und Patch Stand.)
(2) Es dürfen nur vom Auftraggeber zugewiesene Netzwerkanschlüsse verwendet werden.
(3) Die Installation und der Betrieb von aktiven Komponenten (Modem, Router, AccessPoints etc.) im Auftraggebernetzwerk ist untersagt.
(4) Die Installation und/oder die Veränderung von Hard- und Software auf den von SAH bereitgestellten Endgeräten, darf nur nach Rücksprache mit der IT erfolgen.

5. Vorgaben Remote Einwahl

Der Auftragnehmer darf nur die ihm zugewiesene Fern- oder Remote Einwahl verwenden. Eine Remote Einwahl muss durch den IT-Bereich der Stahlwerk Annahütte freigegeben werden. Dem Auftragnehmer stehen folgende Möglichkeiten/Arten zur Verfügung:

(1) SSL VPN
Dem Auftragnehmer wird ein SSL VPN Client zur Verfügung gestellt. Dieser ist auf den Geräten des Auftragnehmers zu installieren.
(2) S2S Verbindung
Zwischen dem Auftragnehmer und dem Auftraggeber wird eine feste und dauerhafte Site-to-Site Verbindung via VPN eingerichtet.

6. Umgang mit Administratorenrechten

Der Auftragnehmer und seine Subunternehmen stellen sicher, dass dortige Mitarbeitern mit Administrationsrechten die folgenden Vorgaben einhalten:

(1) Die Mitarbeiter dürfen die zum Zweck der Erfüllung des Auftrags eingerichteten Administrationsrechte ausschließlich für den vorgesehenen Zweck verwenden. Ihnen ist eine Weitergabe und/oder die Übertragung der zur Erfüllung der Aufgaben persönlich zugeordneten Administrationsrechte sowie diesbezüglicher Benutzerkennungen und Passwörter untersagt.
(2) Räumt der Auftraggeber dem Auftragnehmer aus technischen oder organisatorischen Gründen weitergehende technische Berechtigungen ein, als für die Erfüllung des Auftrags erforderlich, darf der Auftragnehmer und seine Subunternehmer dennoch nur die Berechtigungen nutzen, die zur Erfüllung des Auftrags zwingend benötigt werden.
(3) Jeglicher unberechtigte, insbesondere außerhalb des Auftrags liegende Zugang und Zugriff auf IT-Systeme, Dienste, Daten und Anwendungen des Auftraggebers ist untersagt.
(4) Das Überwinden von Schutzmaßnahmen und Verschlüsselungsmechanismen ist untersagt.

(5) Bei der Durchführung von Administrationsaufgaben muss auf eine strikte Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität der IT-Systeme, Dienste, Daten und Anwendungen geachtet werden.

7. Allgemeine Verpflichtungen

7.1 Meldepflicht, Zugangs- und Zugriffssperrung

Der Auftragnehmer ist verpflichtet, die für ihn einschlägigen Sicherheitsregelungen und Gesetze
einzuhalten, sämtliche relevanten Fehler, Unregelmäßigkeiten oder Sicherheitsvorfälle sowie eingeleitete Maßnahmen zu deren Behebung dem Auftraggeber unverzüglich zu melden.

Sollten diese Sicherheitsrichtlinien nicht eingehalten werden, behält sich der Auftraggeber das Recht vor, den Zugriff des Auftragnehmers und/oder seiner Subunternehmen auf das Netzwerk der Stahlwerk Annahütte ohne vorherige Ankündigung ganz oder teilweise zu sperren.

7.2 Nutzung von Informationen des Auftraggebers

(1) Der Auftragnehmer und seine Subunternehmen sind verpflichtet, die vom Auftraggeber eingeräumten Zugangs-/Zugriffsrechte (IT-Systeme, Dienste, Daten und Anwendungen) ausschließlich im Rahmen ihrer vertraglich zu erfüllenden Verpflichtungen zu nutzen.

(2) Sämtliche durch den Auftrag erlangte, nicht öffentlich bekannte Informationen sowie auftragsbedingt erstellte Kopien, Aufzeichnungen und Arbeitsergebnisse sind Eigentum des Auftraggebers und an diesen nach Beendigung des Auftrages heraus- bzw. zurückzugeben.

(3) Der Auftragnehmer und seine Subunternehmen sind verpflichtet, alle ihm im Zusammenhang mit der Vertragserfüllung zur Kenntnis gelangten Informationen, ihre Geschäfts- und Betriebsangelegenheiten und alle Arbeitsergebnisse vertraulich zu behandeln und angemessen gegen eine Kenntnisnahme durch Unberechtigte und nicht vertragsgemäße Nutzung, Vervielfältigung oder Weitergabe zu schützen. Diese Verpflichtungen gelten über die Beendigung des Vertragsverhältnisses hinaus

(4) Dem Auftragnehmer und seinen Subunternehmen ist nicht gestattet, sich geschäftliche oder betriebliche, nicht öffentlich bekannt gemachte Informationen gleich welcher Art über Auftraggeber und/oder seine Kunden, Lieferanten oder Mitarbeiter anzueignen, für eigene Zwecke zu nutzen oder Kopien oder Aufzeichnungen irgendwelcher Art zu fertigen, soweit dies nicht zur Erfüllung des Auftrags erforderlich ist. Solche Informationen, Kopien, Aufzeichnungen oder Arbeitsergebnisse dürfen auch nicht an Dritte weitergegeben oder Dritten zur Kenntnis gebracht werden.

(5) Vertrauliche Informationen dürfen nur an die Subunternehmen weitergegeben werden, für die der Auftraggeber seine Zustimmung erteilt hat und die auf die Einhaltung der vorliegenden Sicherheitsrichtlinie verpflichtet wurden.

7.3 Datengeheimnis

Der Auftragnehmer darf beim Auftraggeber nur auf das Datengeheimnis (§ 5 BDSG), die Informationssicherheit und ggf. auf sonstige Geheimnisse (u. a. § 88 TKG) verpflichtetes Personal
einsetzen. Die Verpflichtungen gelten auch nach Beendigung der Tätigkeit fort.

7.4 Mitarbeiterqualifikation

Der Auftragnehmer ist verpflichtet, ausschließlich Mitarbeiter einzusetzen, die zur Bearbeitung der zugewiesenen Aufgabe Fachlich ausgebildet sind. Das Gleiche gilt für Mitarbeiter von Subunternehmen.

Die IT Sicherheitsvorgaben erhalten, gelesen und damit einverstanden:

Name des Auftragnehmers: _____

_____ _____

Ort, Datum Unterschrift Auftragnehmer