**Lieferantenbewertung „Informationssicherheit“**

Zur Einhaltung der Informationssicherheitsanforderungen der AMAG Austria Metall AG (kurz AMAG), ist es notwendig die Informationssicherheit von Lieferanten der AMAG zu bewerten und zu überprüfen.

Auf den folgenden Seiten sind die definierten Aussagen auf einer Skala von „trifft vollkommen zu“ bis „trifft überhaupt nicht zu“ zu bewerten.

Bei Vorhandensein einer entsprechenden Zertifizierung bzgl. Informationssicherheit (Informationssicherheitsmanagement-Zertifikat) entfällt die Notwendigkeit zur Bewertung folgender Aussagen. Jedoch ist diesbezüglich ein entsprechender Nachweis (z.B.: ISO27001-Zertifikat, TISAX-Zertifikat/Label, o.ä.) und eine Angabe der Ansprechperson für Informationssicherheit zu erbringen.

Im Rahmen der Einhaltung der allgemeinen Einkaufsbedingungen behält sich AMAG das Recht vor, die Angaben mittels Aufforderung zur Erbringung eines Nachweises zu überprüfen. Sollte die Bewertung nicht durchgeführt oder nicht zufriedenstellend durchgeführt werden, behält sich AMAG weiters das Recht vor, eine Frist zur Umsetzung etwaiger Maßnahmen zu fordern oder die Lieferantenqualifizierung abzubrechen.

Die Rückmeldung der Lieferantenbewertung hat an folgende Email-Adresse zu erfolgen: [Einkauf@amag.at](mailto:Einkauf@amag.at)

**Angaben des Lieferanten:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name:**   |  | | --- | |  |   **Unternehmen:**   |  | | --- | |  |   **Funktion/Rolle:**   |  | | --- | |  |   **E-Mail:**   |  | | --- | |  | |

1. Sie haben ein Informationssicherheitsmanagementsystem implementiert.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben eine Informationssicherheitsrichtlinie bzw. eine Benutzerrichtlinie zur sicheren Nutzung von IT-Systemen und IT-Anwendungen implementiert.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben einen Informationssicherheitsbeauftragten im Unternehmen benannt.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Ihre Mitarbeiter sind hinsichtlich Informationssicherheit ausreichend sensibilisiert und werden regelmäßig geschult.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben Risiken hinsichtlich Informationssicherheit identifiziert, bewertet und geeignete Behandlungsmaßnahmen (z.B.: zur Risikominimierung) abgeleitet.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben zur Fortführung der Geschäftstätigkeit geeignete Business Continuity Pläne implementiert.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben zum Schutz von Informationsverarbeitungsanlagen physische Sicherheitsbereiche definiert und geeignete Überwachungs- und Steuerungsmechanismen implementiert (elektr. Zutrittskontrolle).

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben geeignete Prozesse und Verfahren zur frühzeitigen Erkennung, Auswertung und Behebung von technischen Schwachstellen von IT-Systemen implementiert. Ebenso werden sämtliche IT-Systeme regelmäßig einem Systemaktualisierungsprozess unterzogen.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben flächendeckende technische Schutzmaßnahmen gegen Sicherheitsbedrohungen aus öffentlichen Netzen implementiert (Anti-Viren-Systeme, Firewall, Netzwerk-Authentifizierungs-Kontrollen, Fernzugriffe ausschließlich mit Multi-Faktor-Authentifizierung, etc.).

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben geeignete Prozesse und Verfahren zur frühzeitigen Erkennung und Behandlung von Sicherheitsbedrohungen auf IT-Systeme implementiert (SIEM – Security Information und Event Management, SOC – Security Operation Center, etc.).

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben zum Schutz von Daten und Informationen geeignete Datensicherungsprozesse implementiert (inkl. regelmäßige Wiederherstellungstests und Schutz vor Verschlüsselung von Datensicherungen).

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben ein umfassendes Lieferantenmanagement hinsichtlich Informationssicherheit etabliert und demnach Informationssicherheits-Anforderungen sowie deren Einhaltung vertraglich vereinbart.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

1. Sie haben ein Notfallmanagement zur Vorbereitung und Behandlung von Cyber Krisen (z.B.: Ransomware-Attacken) etabliert. Regelmäßige Krisenübungen werden durchgeführt.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| trifft vollkommen zu | trifft eher zu | trifft eher nicht zu | trifft überhaupt nicht zu |

Ihr Kommentar:

|  |  |  |
| --- | --- | --- |
| Ort/Datum |  | Unterschrift |