

# Lieferantenselbstauskunft zur Informationssicherheit

Supplier self-assessment on its Information Security

## 1.1 Allgemeine Angaben / General Information

- Firmenname / [Company Name](#) \_\_\_\_\_
- Adresse des Standortes / [Location address](#) \_\_\_\_\_
- Branche / [Industry](#) \_\_\_\_\_
- Ansprechpartner/ [Contact person](#) \_\_\_\_\_
- Telefon / [Phone number](#) \_\_\_\_\_
- E-Mail / [E-Mail](#) \_\_\_\_\_
- Anzahl Gesamtbelegschaft / [Number of employees](#) \_\_\_\_\_

## 1.2 Gebäude / Freigelände / Buildings / Open-air area

### 1.2.1 Einfriedung / Hedge

Das Firmengelände ist / The company site is

komplett / completely     teilweise / partly     nicht / not    eingezäunt / hedged.

Die Einfriedung wird komplettiert bis / The hedge will be completed until \_\_\_\_\_.  
Zeitschiene / timeline: \_\_\_\_\_

### 1.2.2 Tore / Zufahrten / Driveway / Access

#### Zutrittsberechtigungskontrolle / Access permission control

	Anzahl / Number	System / System	Personell / Staff	Keine / None
• Personenzugänge / People access	_____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Fahrzeugtore / Vehicle driveway	_____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### 1.2.3 Zutrittskontrolle / Access control

#### Zutrittsberechtigungskontrolle / Access permission control

Bereich / Division	Elektronisch / Electronic <small>(Token, Karte, Pin / Token, Card, Pin)</small>	Personell / Staff	Mechanisch / Mechanical <small>(Schlüssel / Keys)</small>	Keine / None
• Serverraum / Server room	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Datensicherungsarchiv / Backup archive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Prüfstände / Test bench	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Entwicklungsbereiche / Development departments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Prototypenbereich / Prototyping area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Prototypenteilelager / Prototype parts warehouse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Teststrecke / Test track	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
• Produktion / Production	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### 1.2.4 Vergabe von Zutrittsberechtigungen / Assignment of access authorization

**Bereich / Division**

**Verantwortlicher / Responsible Person**

- IT-Bereich / IT Division
- Prototypenbereich / Prototyping area
- Entwicklungsbereich / Projekträume / Development departments / Project rooms
- Produktion / Production

---



---



---



---

### 1.2.5 Schließung / Locking

2.  Es ist eine General- bzw. Hauptschließanlage vorhanden. / A general or main locking system exists.
3. Es sind Schließgruppen vorhanden für / There are lock groups for
 

<input type="checkbox"/> Außentüren / exterior door	<input type="checkbox"/> IT-/ Serverräume / IT-/ Server rooms	<input type="checkbox"/> Entwicklungsbereich/ Projekträume / Development departments / Project rooms	<input type="checkbox"/> Prototypenbereich / Prototyping area
---	---	--	---
4.  Die Schließung hat eine VdS-/EU-Zulassung. / The Locking has a VdS-/EU-certificate.
5.  Es ist ein Schließplan vorhanden. / A locking plan exists.
6.  Es besteht eine zentrale Schlüsselverwaltung. / A central key management exists.
7.  Es ist ein Verantwortlicher für die Schlüsselverwaltung benannt / A responsible person for the key management is named: \_\_\_\_\_
8.  Die Schlüsselausgabe wird dokumentiert. / The key issuing is documented.  
 Art der Dokumentation / Method of documentation: \_\_\_\_\_

### 1.2.6 Einbruchmeldeanlagen / Alarm system

Es ist eine Einbruchmeldeanlage vorhanden. / A burgler alarm system is existing.

Folgende Bereiche werden gesichert / The following divisions are secured:

- IT-Bereich / Serverraum / IT-/ Server rooms
- Prototypenbereich / Prototyping area
- Entwicklungsbereich /Projekträume / Development departments / Project rooms
- Produktion / Production
- Weitere / Further: \_\_\_\_\_

Die Überwachung arbeitet mit folgenden Meldern / The monitoring operates with the following detectors:

- |   |  |   |
|---|--|---|
| <input type="checkbox"/> Bewegungsmelder /<br>Motion detector       | <input type="checkbox"/> Magnetkontakt /<br>Magnetic contact | <input type="checkbox"/> Tür-/Fensterkontakt /<br>Door/window contact       |
| <input type="checkbox"/> Glasbruchsensor /<br>Glass breakage sensor | <input type="checkbox"/> Lichtschranke /<br>Light barrier    | <input type="checkbox"/> Infrarot-/Wärmesensor /<br>Infrared/thermal sensor |

Die Anlage ist aufgeschaltet auf / The System is targeted to:

- |   |   |   |
|---|---|---|
| <input type="checkbox"/> Sicherheitsfirma /<br>Security company | <input type="checkbox"/> Polizei / Police | <input type="checkbox"/> Benachrichtigung an<br>Mitarbeiter / Notification to staff |
| <input type="checkbox"/> Sonstige / Other: _____                |   |   |

- Name und Anschrift der Errichterfirma für Sicherheitstechnik / Name and address of the installation company of the security technology:

Die Einbruchmeldeanlage wurde nach den Richtlinien für Planung und Einbau des VdS<sup>1</sup> bzw. nach EU-Norm installiert / The Alarm System was installed regarding the VdS<sup>1</sup> or EU-Norm directives for planning and installation.  
(DIN VDE 0833-1 und DIN VDE 0833-3 bzw. EN 50131-1).

### 1.3 Fragebogen Informationssicherheit / Deutsch

Allgemeines zum Schutz von Informationen					Auszufüllen durch Heyco			
Nr.	Frage	Ja	Nein	teilweise	Erläuterung	Auszufüllen durch Heyco		
						konform	Nicht k.	Maßnahme
1	Gibt es für Ihr Unternehmen einen Informationssicherheitsbeauftragten?							
2	Haben Sie Ziele für Ihre Informationssicherheit definiert und wurden diese schriftlich fixiert?							
3	Berücksichtigen Sie diese Ziele bei allen neuen Projekten (IT, Facility, Prozessänderungen etc.)?							
4	Haben Sie Sicherheitsrichtlinien definiert für die Nutzung von IT-Geräten, Mail, Internet, Weitergabe von Informationen und Nutzung mobiler IT-Geräte?							
5	Wurden alle Mitarbeiter zu den Richtlinien geschult und zur Einhaltung verpflichtet?							
6	Wird die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüft?							
7	Gibt es eine Richtlinie zur Klassifizierung und Kennzeichnung von Informationen?							
8	Sind Sicherheitszonen schriftlich definiert?							
9	Ist der Zugang zu vertraulichen Informationen nur in einem zugriffsbeschränkten							

Allgemeines zum Schutz von Informationen					Auszufüllen durch Heyco			
Nr.	Frage	Ja	Nein	teilweise	Erläuterung	konform	Nicht k.	Maßnahme
	Sicherheitsbereich möglich?							
10	Ist eine Einsichtnahme von außen in diesen Sicherheitsbereich möglich? Wie wird dies verhindert?							
11	Ist der zutrittsberechtigten Personenkreis beschränkt und dokumentiert?							
12	Haben externen Personen Zutritt zu dem Sicherheitsbereich: <ul style="list-style-type: none"> <li>• Reinigungsdienst,</li> <li>• Wachdienst</li> <li>• Technisches Personal</li> <li>• Weitere</li> </ul>							
13	Werden die Zutritte Externer während der kompletten Zutrittsdauer überwacht?							
14	Ist das Zutrittsmanagement etabliert, dokumentiert und mit klaren Rollen und Zuständigkeiten versehen?							
15	Werden die vergebenen Zutrittsrechte regelmäßig überprüft?							
16	Ist ein Berechtigungsmanagement für den Zugang zu IT-Systemen etabliert und dokumentiert?							
17	Legt eine schriftliche Passwort-Policy die Verwendung starker Passworte (3 aus 4, Länge min. 10 etc.) fest?							
18	Ist der Zugang zu vertraulichen							

Allgemeines zum Schutz von Informationen					Auszufüllen durch Heyco			
Nr.	Frage	Ja	Nein	teilweise	Erläuterung	konform	Nicht k.	Maßnahme
	Informationen ausschließlich mittels starker Authentisierung (2-Faktor) möglich?							
19	Ist die Verwendung mobiler Datenspeicher untersagt? Wird dies kontrolliert bzw. technisch unterbunden?							
20	Sind alle Speicherorte vertraulicher Daten verschlüsselt? Insbesondere: <ul style="list-style-type: none"> <li>• Server / Storage</li> <li>• Backup</li> <li>• Notebook</li> </ul>							
21	Sind die IT-Betriebsabläufe dokumentiert? Werden die administrativen Tätigkeiten protokolliert?							
22	Werden Fernwartungszugänge bei Bedarf von einem Mitarbeiter aktiviert und die Fernwartung überwacht?							
23	Gibt es ein grundsätzliches Foto / Film / Aufnahmeverbot?							
24	Ist ein aktueller Schutz vor Schadsoftware sichergestellt?							
25	Stellt das Patchmanagement eine zeitnahe Aktualisierung von Sicherheitspatches sicher?							
26	Stellt eine Backup-Policy die Verfügbarkeit der Daten inkl. Auslagerung sicher?							

Allgemeines zum Schutz von Informationen					Auszufüllen durch Heyco			
Nr.	Frage	Ja	Nein	teilweise	Erläuterung	Auszufüllen durch Heyco		
						konform	Nicht k.	Maßnahme
27	Ist der Zugriff / Einsicht auf Prototypen während des gesamten Lebenszyklus (Entstehung, Lagerung, Bearbeitung etc. inkl. Vernichtung) nur für berechnigte und mit der HEYCO-WERK Heynen GmbH & Co. KG abgestimmten Personen möglich?				Bitte beschreiben Sie, wie dies gewährleistet wird.			
28	Wird der Transport von Prototypen ausschließlich nach den Vorgaben der HEYCO-WERK Heynen GmbH & Co. KG ausgeführt?				Vorgabe: Blickdichte Verpackung; in neutralem Umkarton versandt.			
29	Stellen Sie sicher, dass jegliche Weitergabe vertraulicher Informationen ausschließlich an Personen erfolgt, die von der HEYCO-WERK Heynen GmbH & Co. KG autorisiert sind?							
30	Erfolgt eine autorisierte Weitergabe ausschließlich in verschlüsselter Form, bei der der Schlüssel auf separatem physischen Weg übertragen wird?							
31	Sind alle evtl. genutzten Cloud-Dienste inkl. Conferencing- und Fernsteuerungslösungen, die vertrauliche Daten enthalten können von der HEYCO-WERK Heynen GmbH & Co. KG geprüft und freigegeben?							



Allgemeines zum Schutz von Informationen					Auszufüllen durch Heyco		
Nr.	Frage	Ja	Nein	teilweise	Erläuterung	Auszufüllen durch Heyco	
						konform	Nicht k.
32	Sind alle Ihre Unterauftragnehmer der HEYCO-WERK Heynen GmbH & Co. KG angezeigt und von dieser freigegeben?						
33	Beinhalten die vertraglichen Vereinbarungen zwischen Ihnen und Ihren Unterauftragnehmern dieselben Bestimmungen zur Informationssicherheit, wie Ihr Vertrag mit der HEYCO-WERK Heynen GmbH & Co. KG?						
34	Melden Sie alle Informationssicherheitsereignisse dem Informationssicherheitsbeauftragten der HEYCO-WERK Heynen GmbH & Co. KG?						

### 1.3 Questionnaire Information security / English

General questions regarding the protection of information					Filled by HEYCO			
Nr.	Question	Yes	No	Partly	Explanations	Compliant	Not compliant	Actions
1	Does your company have an Information Security Representative?							
2	Did you define and document goals for your information security?							
3	Do you take these goals into account in all your new projects (IT, facility, process changes etc.)?							
4	Did you define security directives for the use of IT-devices, mails, internet, transfer of information and usage of mobile IT-devices?							
5	Were all employees trained and bound to compliance regarding the directives?							
6	Does the effectiveness of the security actions get examined regularly?							
7	Does a directive for classification and notation of information exist?							
8	Did you define and document security zones?							
9	Is the access to confidential information only in restricted security areas possible?							
10	Is an inspection from outside possible? How do you prevent this?							
11	Is the authorized group of persons limited and documented?							

General questions regarding the protection of information						Filled by HEYCO		
Nr.	Question	Yes	No	Partly	Explanations	Compliant	Not compliant	Actions
12	Do external persons have access to the security area: <ul style="list-style-type: none"> <li>• Cleaning service,</li> <li>• Security</li> <li>• Technical staff</li> <li>• Further</li> </ul>							
13	Is the access of externals during their whole access time monitored?							
14	Is an access management established, documented and clear roles and responsibilities defined?							
15	Are the assigned access rights regularly reviewed?							
16	Is an authorization management for the access to the IT-systems established and documented?							
17	Does a written password policy state the usage of strong passwords (3 out of 4, length min. 10, etc.)?							
18	Is the access to confidential information only possible through a strong authentication (2-factor)?							
19	Is the usage of mobile data storage forbidden? Is this controlled or technically prevented?							
20	Are all storage locations of confidential data encrypted? Especially: <ul style="list-style-type: none"> <li>• Server / Storage</li> </ul>							

General questions regarding the protection of information					Filled by HEYCO			
Nr.	Question	Yes	No	Partly	Explanations	Compliant	Not compliant	Actions
	<ul style="list-style-type: none"> <li>• Backup</li> <li>• Notebook</li> </ul>							
21	Are the IT-processes documented? Are the administrative activities documented?							
22	Is the remote maintenance access activated, if required, by a staff member and is the remote maintenance monitored?							
23	Do you have a general photo / film / recording ban?							
24	Is a latest protection of malware ensured?							
25	Does the patch management ensure the prompt updating of security patches?							
26	Does a backup policy ensure the availability of information including the outsourcing?							
27	Is the access / insight to prototypes during the whole life cycle (development, storage, processing, etc. incl. destruction) only possible for persons who are authorized by HEYCO-WERK Heynen GmbH & Co. KG?				Please describe how this will be ensured.			
28	Is the transport of prototypes solely performed in accordance to the specifications of the HEYCO-WERK				Specification: opaquely packed; sent in a neutral carton.			

General questions regarding the protection of information						Filled by HEYCO		
Nr.	Question	Yes	No	Partly	Explanations	Compliant	Not compliant	Actions
	Heynen GmbH & Co. KG?							
29	Do you secure, that confidential information is solely transferred to persons, that are authorized by the HEYCO-WERK Heynen GmbH & Co. KG?							
30	Does the authorized transfer solely take place encrypted and is the key then sent through a separate physical way?							
31	Are all potential used cloud services, incl. conferencing- and remote control solutions, which could contain confidential information reviewed and authorized by the HEYCO-WERK Heynen GmbH & Co. KG?							
32	Are all your subcontractors displayed to the HEYCO-WERK Heynen GmbH & Co. KG and authorized from it?							
33	Do the contractual agreement between you and your subcontractor contain the same regulations regarding information security as your contract with the HEYCO-WERK Heynen GmbH & Co. KG?							
34	Do you report all information security incidents to the information security representative of the HEYCO-WERK Heynen GmbH & Co. KG?							





## 2. Prozessdokumentation / Process documentation

### 2.1 Selbstauskunft / Self-assessment

Hiermit bestätigen wir die Richtigkeit der Angaben der Selbstauskunft. / We hereby confirm the correctness of the statements in this self-assessment.

Lieferant / Supplier:

---

Datum  
Date

Name, Funktion  
Name, Role

Unterschrift  
Signature