

Bestätigung der Informationssicherheit Technische und organisatorische Maßnahmen

Die hmp HEIDENHAIN MICROPRINT GmbH stellt bei der Verarbeitung von Daten die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten sicher.

1. Vertraulichkeit

Es wird sichergestellt, dass keinen unbefugten Dritten Zugriff oder Zugang zu schützenswerten Daten oder Systemen haben.

2. Integrität

Es wird sichergestellt, dass keine unbefugten Dritten relevante Daten oder Systeme unbemerkt verändern oder löschen können.

3. Verfügbarkeit und Belastbarkeit

Es wird sichergestellt, dass relevante Daten oder Systeme zum Zeitpunkt, zu dem sie benötigt werden, zur Verfügung stehen bzw. rechtzeitig wiederhergestellt werden können.

4. Verfahren zu regelmäßiger Überprüfung, Bewertung und Evaluierung

Es wird sichergestellt, dass Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung vorhanden sind.

5. Schutzmaßnahmen

Im Nachfolgenden werden getroffene Schutzmaßnahmen zur Einhaltung oben genannter Schutzziele erläutert.

5.1 Organisation

- Innerhalb der Organisation sind Verantwortlichkeiten definiert, die informationssicherheitsrelevante Aufgabenbereiche und Funktionen koordinieren.
- Anforderungen an die Informationssicherheit werden regelmäßig überprüft und neu bewertet.
- Werden Dritte mit Aufgaben an schutzrelevanten Daten oder Systemen beauftragt, so wird das Risiko bewertet und angemessene Maßnahmen umgesetzt.

5.2 Management von organisationseigenen Werten

- Alle kritischen organisationseigenen Werte sind eindeutig identifizierbar und in einer Inventarverwaltung gepflegt.
- Es sind Prozesse definiert, die die Aktualität der kritischen Werte sicherstellt.
- Es sind Regelungen und Vorgaben für den zulässigen Gebrauch von organisationseigenen Assets vorhanden.

5.3 Personelle Sicherheit

- Schutzrelevante Themen werden im Rahmen der Arbeitsverträge geregelt.
- Mitarbeiter werden während Ihrer Anstellung regelmäßig bezüglich Informationssicherheit sensibilisiert.
- Organisationseigene Assets werden bei Beendigung des Arbeitsverhältnisses zurückgegeben.
- Zugangs- und Zugriffsberechtigungen werden bei Beendigung des Arbeitsverhältnisses entzogen.

5.4 Physische Sicherheit / Zutrittskontrolle

- Es sind Sicherheitszonen eingerichtet, die mit entsprechendem Zugangsschutz gesichert sind.
- Besucher müssen sich am Empfang melden. Sie werden registriert und erhalten einen Besucherausweis.
- Das Werksgelände ist durch einen Zaun und Videoüberwachung geschützt.
- Das Rechenzentrum ist durch einen erweiterten Zutrittsschutz gesichert.
- Physische Schutzmaßnahmen vor Bedrohungen von außen oder aus der Umgebung wie Feuer, Vandalismus oder ähnliches wurden getroffen.
- Relevante datenverarbeitende Systeme sind vor Stromausfällen oder anderen Versorgungseinrichtungen entsprechend geschützt.
- Datenverarbeitende Systeme werden entsprechend gewartet.
- Es gibt Regelungen für die erlaubte Entfernung von Assets aus dem Betriebsgelände.

5.5 Betriebs- und Kommunikationsmanagement / Weitergabekontrolle

- Für definierte Systeme sind dokumentierte Betriebsprozesse vorhanden. Dies beinhaltet z. B. Dokumente über Backup, Betrieb oder Ansprechpartner der jeweiligen Systeme.
- Änderungen an informationsverarbeitenden Einrichtungen werden geregelt durchgeführt.
- Für definierte Systeme sind getrennte Test- und Produktivsysteme vorhanden.
- Kapazitäten von definierten informationsverarbeitenden Systemen werden geplant und überwacht.
- Neue informationsverarbeitende Systeme werden nach einem definierten Prozess freigegeben.
- Maßnahmen gegen Schadsoftware wie Virens Scanner und Firewalls wurden getroffen.
- Für definierte informationsverarbeitende Systeme wurde ein entsprechendes Backupkonzept definiert und etabliert.
- Für datenverarbeitende Netze wurden Maßnahmen definiert, um die übertragenen Informationen zu schützen.
- Für den Umgang mit Wechselmedien sind entsprechende Verfahrensanweisungen vorhanden.
- Betriebsmittel werden sicher außer Betrieb genommen, d. h. persistente Speicher von relevanten Informationen sicher gelöscht bzw. zerstört.
- Es gibt formale Regelungen, wie Informationen zu speichern bzw. weiterzugeben sind.
- Es gibt Regelungen, wie Informationen zu vernichten sind.
- Es stehen Maßnahmen zur Verfügung, um Informationen im Zuge eines Datenaustausches zu schützen.
- Werden Daten zwischen Organisationen ausgetauscht, so werden entsprechende Vereinbarungen getroffen.
- Die Nutzung definierter Informationssysteme wird überwacht und der Zugriff auf diese Logs entsprechend eingeschränkt.
- Definierte Informationssysteme unterliegen einer zentralen Zeitsynchronisation.

5.6 Zugangs- und Zugriffskontrolle

- Die Vergabe, die Änderung und der Entzug von Berechtigungen erfolgt nach einem definierten Prozess (abgestufte Zugriffsberechtigung).
- Die organisatorische Berechtigungsbewilligung (z. B. durch den Vorgesetzten) und die technische Berechtigungsvergabe (durch IT) erfolgen durch verschiedene Personen.
- Die Vergabe, Änderung und der Entzug von Berechtigungen wird dokumentiert.
- Sonderrechte werden nur eingeschränkt und kontrolliert vergeben.
- Passwörter von Benutzern werden nach einem definierten Prozess ausgegeben.
- Arbeitsplatzrechner sind nur über eine Benutzeranmeldung mit persönlichem Passwort zugänglich.
- Es gibt Anweisungen zum ausreichenden Schutz unbeaufsichtigter Benutzerausstattung.
- Jeder Benutzer verfügt über eine eindeutige Benutzerkennung.
- Der Zugriff auf Informationen ist eingeschränkt.

5.7 Beschaffung, Entwicklung und Wartung von Informationssystemen

- Anforderungen an Sicherheitsmaßnahmen werden spezifiziert.
- Es gibt dokumentierte Leitlinien für den Einsatz von Kryptographie.
- Der Anwender wird bei der Schlüsselverwaltung durch geeignete Werkzeuge unterstützt.
- Für die Freigabe von Software für den Betrieb ist ein geeigneter Prozess etabliert.
- Änderungen an Informationssystemen werden dokumentiert und in geeigneter Weise dem User zur Verfügung gestellt.
- Änderungen an Informationssystemen werden vor Freigabe durch definierte User getestet.

5.8 Umgang mit Informationssicherheitsvorfällen

- Schwachstellen an Informationssystemen und Software werden gemanagt.
- Es gibt definierte Prozesse Informationssicherheitsvorfälle zu melden.

5.9 Einhaltung von Vorgaben

- Anwendbare Gesetze und Vorgaben werden identifiziert.
- Die Vertraulichkeit von Informationen wird sichergestellt.
- Die Einhaltung von Vorgaben wird geprüft.

Stand: März 2026