Cybersicherheit und Informationstechnologie

1 Inhaltsverzeichnis

Knott GmbH · Standort Eggstätt · Obinger Straße 15 · 83125 Eggstätt · Tel. +49 8056 906-0 · info@knott.de · www.knott.de
Standort Regenstauf · Gutenbergstraße 21 · 93128 Regenstauf · Tel. +49 9402 9317-0 · shop@knott.de · www.knott.de
Vorlagenverantwortlicher tli · **Datum** 29.08.2025 · **Version** 001

Cybersicherheit und Informationstechnologie

2 Zweck und Zielsetzung

Diese Werksnorm definiert die verbindlichen Anforderungen zur Absicherung von IT-Systemen bei allen Lieferanten von Knott. Ziel ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit der von Lieferanten verarbeiteten Informationen, die im Zusammenhang mit Geschäftsprozessen von Knott stehen.

3 Geltungsbereich

Diese Werksnorm gilt für:

- alle IT-Systeme (Server, Clients, mobile Endgeräte, Cloud-Services),
- alle Netzwerke und Kommunikationssysteme,
- alle physischen und virtuellen Umgebungen,
- alle Subunternehmer und Partner, die durch den Lieferanten eingebunden werden

4 Allgemeine Anforderungen

- Lieferanten müssen ein angemessenes Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 oder gleichwertigen Standards betreiben
- Es sind Risikobewertungen durchzuführen und dokumentiert bereitzustellen
- Ein Sicherheitsbeauftragter muss benannt sein

5 Technische Sicherheitsanforderungen

5.1 Zugriffsschutz

- Systeme sind durch starke Authentifizierung (mindestens Multifaktorauthentifizierung (MFA) bei Fernzugriff) abzusichern.
- Passwortrichtlinien: z.B. Komplexität, regelmäßige Änderung bei Verdacht auf Kompromittierung
- Rechtevergabe nach dem Need-to-know-Prinzip
- Privileged Access Management (PAM) oder Mindestanforderung für Admin-Konten
- Logging von Anmeldeversuchen / Zugriffen

5.2 Verschlüsselung

- Transportverschlüsselung (ist verpflichtend für alle Datenübertragungen)
- Speicherverschlüsselung für mobile Geräte, Laptops, externe Datenträger und Cloud-Speicher
- Schlüsselmanagement muss dokumentiert und sicher umgesetzt sein

5.3 Systemhärtung

- Systeme müssen nach anerkannten Best Practices (z. B. Bundesamt für Sicherheit in der Informationstechnik (BSI) Grundschutz) gehärtet werden
- Standard-Passwörter und unnötige Dienste sind zu entfernen/deaktivieren
- Sicherheitsupdates und kritische Patches müssen zeitnah installiert werden
- Endpoint Detection & Response für erweiterte Angriffserkennung ist einzusetzen

Knott GmbH · Standort Eggstätt · Obinger Straße 15 · 83125 Eggstätt · Tel. +49 8056 906-0 · info@knott.de · www.knott.de
Standort Regenstauf · Gutenbergstraße 21 · 93128 Regenstauf · Tel. +49 9402 9317-0 · shop@knott.de · www.knott.de
Vorlagenverantwortlicher tli · **Datum** 29.08.2025 · **Version** 001

Cybersicherheit und Informationstechnologie

5.4 Backup & Recovery

- Regelmäßige Backups (mindestens täglich für kritische Systeme)
- Backups sind verschlüsselt und getrennt vom Produktivsystem aufzubewahren
- Wiederherstellungstests sind mindestens jährlich durchzuführen und nachweisbar zu dokumentieren

5.5 Netzwerk & Kommunikation

- Einsatz von Firewalls, IDS/IPS an allen externen Übergängen (Intrusion Detection System (IDS); Intrusion Prevention System (IPS))
- Netzwerksegmentierung zwischen Produktions-, Verwaltungs- und externen Netzen
- VPN (Virtual Private Network) mit starker Verschlüsselung für Remote-Zugriffe
- Monitoring der IT-Infrastruktur

5.6 Malware- & Angriffsschutz

- Alle Systeme müssen mit aktuellen Anti-Malware-Lösungen ausgestattet sein
- E-Mail-Schutz (Spamfilter, Sandboxing) ist einzusetzen
- SOC/SIEM Logging für sicherheitsrelevante Ereignisse mit entsprechender Aufbewahrung sollte eingesetzt werden (Security Operations Center (SOC) / Security Information and Event Management (SIEM))

6 Organisatorische Anforderungen

6.1 Notfallmanagement

Lieferanten müssen ein dokumentiertes Notfall- und Incident-Response-Konzept vorweisen
Sicherheitsvorfälle sind unverzüglich an Knott zu melden.

6.2 Schulung & Sensibilisierung

Mitarbeiter sind regelmäßig (mindestens 1x jährlich) in IT-Security zu schulen;
Schulungsnachweise sind auf Anfrage vorzulegen

6.3 Audits & Nachweise

Knott behält sich Audits beim Lieferanten oder die Anforderungen von Nachweisen vor
Bei Nicht-Einhaltung können Sanktionen bis hin zur Vertragskündigung erfolgen

7 Verantwortlichkeiten

- Lieferant: Einhaltung und Umsetzung dieser Werksnorm
- Knott: Überwachung, Auditierung und Bereitstellung von Eskalationswegen

8 Inkrafttreten und Überprüfung

- Diese Werksnorm tritt ab dem 01.09.2025 in Kraft
- Sie wird jährlich überprüft und bei Bedarf angepasst

Knott GmbH · Standort Eggstätt · Obinger Straße 15 · 83125 Eggstätt · Tel. +49 8056 906-0 · info@knott.de · www.knott.de
Standort Regenstauf · Gutenbergstraße 21 · 93128 Regenstauf · Tel. +49 9402 9317-0 · shop@knott.de · www.knott.de
Vorlagenverantwortlicher tli · **Datum** 29.08.2025 · **Version** 001