Cyber-Security-Policy (Fassung 2026)

Stürmer-SysTec GbR

Stand: Januar 2026

Diese Cyber-Security-Policy regelt die Grundsätze, Maßnahmen und Sicherheitsanforderungen der Stürmer-SysTec GbR im Umgang mit IT-Systemen, Kundensystemen, Daten und Netzwerken.

---

§1 Zweck und Anwendungsbereich

(1) Die Policy gilt für alle Mitarbeiter, Partner, Subunternehmer und technische Dienstleister der Stürmer-SysTec GbR.

(2) Sie dient der Sicherstellung der Sicherheit von Informationen, Systemen, Daten, Anwendungen, Netzwerken und Services, einschließlich Kundensystemen, die durch Stürmer-SysTec betreut oder administriert werden.

(3) Die Policy gilt für alle IT-Betriebsformen:

- On-Premise
- Cloud
- Remote-Service
- hybride Architekturen
- virtuelle Infrastruktur

---

§2 Grundprinzip der Informationssicherheit

Stürmer-SysTec verpflichtet sich, angemessene technische und organisatorische Maßnahmen zur Sicherstellung von:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Nachvollziehbarkeit

  von Informationen und IT-Systemen zu ergreifen.

---

§3 Zugriffskontrolle

(1) Systemzugriffe erfolgen ausschließlich nach dem „Need-to-Know“- und „Least-Privilege“-Prinzip.

(2) Für alle Benutzerkonten gilt:

- individuelle Benutzer
- keine Konten ohne Passwort
- Passwort-Richtlinien
- regelmäßige Passwort-Änderung
- Dokumentation von Benutzerrechten

(3) Admin-Konten werden ausschließlich nach vorheriger Freigabe genutzt.

---

§4 Verschlüsselung

(1) Datenübertragungen erfolgen ausschließlich verschlüsselt (TLS, VPN, SSH), sofern technisch umsetzbar.

(2) Remote-Zugriffe werden grundsätzlich per VPN oder vergleichbaren Sicherheitsmechanismen durchgeführt.

---

§5 Umgang mit Kundensystemen

(1) Der Zugriff auf Kundensysteme erfolgt ausschließlich nach vorheriger Zustimmung des Kunden oder aufgrund vertraglicher Vereinbarungen.

(2) Zugriffe werden protokolliert.

(3) Daten von Kunden werden nicht ohne Einwilligung außerhalb der Kundensysteme gespeichert, sofern dies nicht vertraglich vereinbart ist.

---

§6 Sicherheitsupdates und Patching

(1) Sicherheitsupdates werden gemäß Herstellervorgaben durchgeführt.

(2) Kritische Sicherheitsupdates können sofort eingespielt werden, sofern ein akuter Sicherheitsbedarf besteht.

---

§7 Malware- und Angriffsschutz

(1) Stürmer-SysTec setzt branchenübliche Viren-, Malware-, Firewall- und Angriffsschutzsysteme ein.

(2) Warnungen, sicherheitskritische Ereignisse und Bedrohungen werden bewertet und im Bedarfsfall Kunden mitgeteilt.

---

§8 Incident-Management

(1) Sicherheitsrelevante Ereignisse werden unverzüglich untersucht, bewertet und dokumentiert.

(2) Bei Sicherheitsvorfällen in Kundensystemen wird der Kunde informiert, sofern dies zur Gefahrenabwehr erforderlich ist.

---

§9 Nutzung externer IT-Dienstleister

Bei Einbindung von Subunternehmern wird die Einhaltung dieser Cyber-Security-Policy vertraglich und organisatorisch sichergestellt.

---

§10 Mobile Arbeit / Remote-Work

(1) Remote-Zugriffe erfolgen ausschließlich über autorisierte Systeme.

(2) Private Geräte dürfen nur genutzt werden, wenn diese Sicherheitsanforderungen erfüllen oder durch Stürmer-SysTec freigegeben wurden.

---

§11 Cloud-Dienste und SaaS

(1) Der Einsatz von Cloud-Diensten erfolgt ausschließlich unter Einhaltung der DSGVO.

(2) Kundendaten werden nur verarbeitet, wenn ein rechtlicher Rahmen besteht (z. B. AV-Vertrag, Auftragsverarbeitung).

Dipl.-Wirt.-Ing. (FH) Stefanie Stürmer
Dipl.-Ing. (FH) Sascha Stürmer
Stürmer-SysTec GbR, Sperberstr. 10, 40627 Düsseldorf

§12 Protokollierung

(1) Sicherheitsrelevante Vorgänge (u. a. Zugriffe, Updates, Remote-Sessions) werden protokolliert.

(2) Logs werden gemäß gesetzlichen Vorgaben aufbewahrt.

---

§13 Datensicherung

(1) Backups für Kundensysteme erfolgen nur auf Basis schriftlicher Vereinbarung.

(2) Ohne gesonderten Vertrag bleibt die Sicherstellung von Backups Aufgabe des Kunden.

---

§14 Meldung von Sicherheitsereignissen

Mitarbeiter und Dienstleister müssen sicherheitsrelevante Ereignisse unverzüglich an die Geschäftsführung melden.

---

§15 Schulung und Sensibilisierung

Stürmer-SysTec vermittelt Mitarbeitern regelmäßig sicherheitsrelevante Informationen, Anweisungen und Richtlinien.

---

§16 Sanktionen und Haftung

Verstöße gegen diese Cyber-Security-Policy können arbeitsrechtliche Maßnahmen und vertragliche Konsequenzen nach sich ziehen.

---

§17 Änderungen der Policy

Stürmer-SysTec behält sich vor, diese Policy bei technischen oder rechtlichen Änderungen jederzeit anzupassen.

Dipl.-Wirt.-Ing. (FH) Stefanie Stürmer
Dipl.-Ing. (FH) Sascha Stürmer
Stürmer-SysTec GbR, Sperberstr. 10, 40627 Düsseldorf

Stürmer Systec
IT CONSULTING