-öffentlich-

Vorgaben zur Informationssicherheit für Auftragnehmer und externe Stellen

---

Paletti
Gewerbepark Meißen 17
32423 Minden

Version 1.0
Stand: 29.11.2019

Inhalt

1. Geltungsbereich

Vorgaben zur Informationssicherheit für Auftragnehmer und externe Stellen gilt für alle Kunden, Auftragnehmer, Besucher, Lieferanten und weitere externe Stellen bei der Zusammenarbeit mit Paletti. Diese Vorgaben gelten an allen Standorten von Paletti sowie allen Standorten des jeweiligen Geschäftspartners.

2. Ziele

Ziel dieser Vorgabe ist es, ein gleichbleibend hohes Niveau zum Schutz von Daten, Informationen und weiterer Informationssicherheitswerte bei Paletti und beim Geschäftspartner zu erreichen

3. Informationssicherheit auf den Geländebereichen von Paletti

Besuchern von Paletti ist es untersagt, sich ohne den zuständigen Ansprechpartner oder zugewiesenen Begleiter in den Gebäuden von Paletti aufzuhalten.
Der Zutritt zu allen Bereichen ist durch den zuständigen Ansprechpartner oder zugewiesenen Begleiter zu autorisieren. Für alle Besucher gelten ergänzend zu dieser Richtlinie die „*allg. Besucherregeln*“.

3.1 Fotografierverbot

Auf dem gesamten Gelände von Paletti gilt das allgemeine Fotografier und Filmverbot.

3.1.1 Ausnahmeregelung

Kunden ist es gestattet, Fotografien im Rahmen ihres eigenen Projektes anzufertigen. Bei der Aufnahme ist darauf zu achten, dass die Vertraulichkeit nicht zum Projekt gehöriger Informationen gewahrt bleibt. Rückfragen hierzu sind an den zuständigen Ansprechpartner zu richten.

Lieferanten ist es gestattet, Aufnahmen von Transportschäden oder mangelhaften Waren anzufertigen.

4. Verarbeitung von Daten und Informationen

Ist es im Rahmen der Zusammenarbeit erforderlich, dass Daten und Informationen ausgetauscht werden, so sind die folgenden Regelungen unbedingt zu beachten.
Dokumente, die von Paletti erzeugt werden, tragen immer eine Kennzeichnung zur Vertraulichkeitsstufe (intern oder vertraulich, nicht gekennzeichnete Dokumente sind als öffentlich zu verstehen). Dokumente, die von Kunden von Paletti bereitgestellt werden, tragen in der Regel eine Kennzeichnung der Vertraulichkeitsstufe des Kunden. Weitere Klassifizierung von Daten und Informationen ergeben sich aus dem Lastenheft der Projekte.

4.1 Austausch von Daten und Informationen

Klassifizierung	Austausch	Ablage auf Mobilen Datenträgern	Vernichtung
Öffentlich	Kein Vorgabe	Keine Vorgabe	Keine Vorgabe
Intern	Daten sollten nach Möglichkeit verschlüsselt *) übermittelt werden (paletti-Cloud, Verschlüsselte E-Mail/E-Mailanhänge, Kundeportal).	Datenträger sollten nach Stand der Technik verschlüsselt werden. **)	Interne Akten sollten nach Möglichkeit im Shredder entsorgt werden.
Vertraulich	Daten sind ausschließlich verschlüsselt *) zu übermitteln (paletti-Cloud, Verschlüsselte E-Mail/E-Mailanhänge, Kundeportal)	Datenträger sind nach Stand der Technik zu verschlüsseln. **)	Informationen in Papierform sind im Schredder (mindestens Sicherheitsstufe P4) zu vernichten

*) E-Mail Verschlüsselung (S/MIME oder PGP), Verschlüsselungsfunktion moderner Firewalls, keine Trivialkennwörter (Firmenname und Jahreszahl, etc.)
**) mindestens AES-256

4.2 Aufbewahrung und Löschung

Daten und Informationen in Zusammenhang mit Projekten von Paletti-Kunden sind gem. der Vereinbarungen in Lastenheften aufzubewahren und zu vernichten.

Daten und Informationen ohne festgelegte Aufbewahrungsfrist in Lastenheften (oder anderen Dokumenten), sind unter Berücksichtigung der gesetzlichen Vorgaben oder entsprechend vertraglicher Regelungen nach Zweckerfüllung unmittelbar zu löschen/vernichten.

Alle Daten und Informationen von Paletti sind von Empfängern immer vor Verletzung der Vertraulichkeit, Verfügbarkeit und Integrität zu schützen.

5. Arbeiten an Paletti IT Systemen

5.1 Regelungen für Auftragnehmer mit Zugriff auf IT-Systeme

- Das unrechtmäßige Abrufen oder Verbreiten von Inhalten, die urheberrechtlich oder datenschutzrechtlich geschützt sind, ist untersagt.
- Das unrechtmäßige Abrufen oder verbreiten von Informationen mit der Schutzstufe Intern oder höher ist untersagt.
- Alle innerhalb der IT-Systeme von Paletti eingesetzte Hard- und Software wird vor ihrem Einsatz durch die Leitung der IT freigegeben.
- Das Herunterladen von Software sowie die Installation oder die Verwendung nicht freigegebener Hard- und Software ist Auftragnehmern nicht gestattet.
- Der Zugriff auf das Internet oder auf Netzwerke, die nicht vom Unternehmen betrieben werden, erfolgt grundsätzlich nur über die vom Unternehmen speziell dafür bereitgestellten Zugänge.

- Zugangskennungen für die Nutzung der IT-Infrastruktur (wie z. B. Benutzernamen und Passwörter) sind vom Auftragnehmer geheim zu halten und dürfen grundsätzlich nicht weitergegeben werden.
    - Auch innerhalb der Organisation des Auftragnehmers ist dieser verpflichtet, die Daten vor anderen Mitarbeitern des Auftragnehmers geheim zu halten. Ausnahmen von dieser Regelung dürfen durch die Leitung IT genehmigt werden, wenn die Leistungen des Auftragnehmers von einem mehrköpfigen Team erbracht werden und eine Personalisierung der Zugangskennungen technisch unmöglich oder wirtschaftlich nicht angemessen ist, sowie ein vergleichbarer Nachweis über die Verwendung der Zugänge vorliegt.
- Die private Nutzung von IT-Systemen von Paletti ist jedem Auftragnehmer untersagt.
- Das eigenmächtige Verschlüsseln oder das Schützen gegen den lesenden Zugriff von Daten durch den Auftragnehmer ist untersagt. Oben genannte Regelungen stehen diesem Punkt nicht entgegen.
- Werden Änderungen an den Sicherheitseinrichtungen vorgenommen oder sollen Netzwerkübergänge (z.B. VPN) eingerichtet werden, so ist dies im Vorfeld mit der Leitung der IT abzustimmen.

5.2 Regelungen für den Einsatz von IT-Systemen des Auftragnehmers

Bei einem Einsatz von IT-Systemen des Auftragnehmers müssen diese über die folgenden Basis-Sicherheitsmaßnahmen verfügen:

- Die IT-Systeme müssen über die notwendigen Lizenzen verfügen.
- Die IT-Systeme müssen ausreichend vor Schadsoftware geschützt sein. Es ist eine Endpoint-Protection zu verwenden, der eine tagesaktuelle Versorgung mit Updates gewährleistet.
- Die Betriebssysteme auf den IT-Systemen müssen dem jeweils aktuellen Stand von Sicherheitsupdates des jeweiligen Betriebssystemanbieters entsprechen. Es sind nur Betriebssysteme zu verwenden, die vom Hersteller noch unterstützt und gepflegt werden.

5.3 Integration von IT-Systemen

Sollen IT-Systeme von Auftragnehmern in die IT-Infrastruktur von Paletti integriert werden, muss zunächst eine Prüfung der Voraussetzungen durch die IT-Administration sowie eine Freigabe durch die Leitung IT erfolgen. Hierzu gelten folgende Anforderungen:

- Der Auftragnehmer legt hierzu die notwendige, aktuelle Dokumentation der betroffenen IT-Systeme vor.
- Der Auftragnehmer hat für seine IT-Systeme ein Datenschutz- und Informationssicherheitskonzept vorzulegen, welches die Maßnahmen zur Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität nachvollziehbar darlegt.

5.4. Umgang mit Daten und Datenträgern

- Alle Daten von Paletti bleiben grundsätzlich innerhalb der IT-Infrastruktur des Unternehmens. Sie dürfen nicht durch Auftragnehmer auf Datenträger oder in andere IT-Systeme übertragen werden.
- Wird im Rahmen der Leistungserbringung des Auftragnehmers ein externer Datenträger benötigt, so muss dieser durch den zuständigen IT-Administrator vor der Verwendung freigegeben werden.
- Im Rahmen dieser Freigabe erfolgt eine Überprüfung des Datenträgers auf Schadsoftware.
- Externe Datenträger, auf denen Unternehmensdaten gespeichert sind, werden grundsätzlich vertraulich behandelt und nach Stand der Technik (mindestens AES-256) verschlüsselt, sofern Informationen ab Schutzstufe „vertraulich“ dort gespeichert werden.
- Externe Datenträger werden nicht an Dritte bzw. unberechtigte Personen weitergegeben.

6. Verhalten bei Informationssicherheitsvorfällen

Sollte im Rahmen der Zusammenarbeit mit Paletti ein Datenschutz – oder Informationssicherheitsvorfall eintreten, so ist dies umgehend (spätestens eine Stunde nach Feststellung) an das Datenschutz- und Informationssicherheitsteam (DIST) von Paletti zu melden. Die Meldung hat per E-Mail oder per Telefon (sofern E-Mail nicht möglich ist) zu erfolgen. Auch bei Verdacht ist umgehend eine Meldung durchzuführen.

Kontaktdaten:

	E-Mail	Telefon:
DIST	dist@paletti.de	-
IT-Leitung	axmann.folker@paletti.de	0571 / 387303 – 69
Geschäftsführung	kahl.helmuth@paletti.de	0571 / 387303 – 0

Beispiele für einen Datenschutz und Informationssicherheitsvorfall können sein:

- Verlust von Datenträgern, Dokumenten oder Geräten mit Paletti-Informationen
- Verletzung (oder Verdacht auf Verletzung) der Vertraulichkeit durch Ausspähen (z.B. im Zug)
- Schadsoftware-Befall
- Verletzung der in diesem Dokument niedergeschriebenen Regelungen
- Feststellung von unbefugtem Zutritt zu Paletti-Räumlichkeiten oder eigenen Räumlichkeiten
- Fehlgeleitetet E-Mails
- etc.

7. Geltung, Evaluierung und Anpassung

Diese Vorgaben sind Bestandteil des ISMS von Paletti und werden regelmäßig überprüft und ergänzt. Die aktuelle Version steht immer auf der Website zum Download zur Verfügung, liegt in allen Paletti Standorten aus und kann auf Nachfrage bei Ihrem Paletti Ansprechpartner angefordert werden.

Stand: 29.11.2019

Änderungsindex

Version	Datum	Beschreibung	Name
1.0	28.11.2019	Initiale Erstellung des Dokuments	Axmann
	29.11.2019	Freigabe durch DIST	DIST
1.0	29.11.2010	Freigabe durch Geschäftsleitung	H. Kahl