Informationssicherheitsrichtlinie
Regelungen für alle Auftragnehmer
der
SCHULZ Systemtechnik GmbH

Hinweis:

Um den Lesefluss nicht zu beeinträchtigen, wird hier nur die männliche Form genannt, doch wird die weibliche Form gleichermaßen mitgemeint.

Inhaltsverzeichnis

1 Zweck dieses Dokumentes und dessen Geltungsbereich

Diese Richtlinie beschreibt die Regelungen für alle Auftragnehmer der SCHULZ Systemtechnik GmbH und deren Mitarbeiter.

2 Umgang mit Informationen der SCHULZ Systemtechnik GmbH

Informationen sind wichtige Werte für unsere Arbeit. Darum müssen wir sorgfältig auf unsere Informationen achten und diese schützen. Dazu gehört unter anderem:

- Alle Informationen sind zu klassifizieren und zu kennzeichnen.
- Vertrauliche Informationen dürfen nur an befugte Personen weitergeben werden.
- Es dürfen nur von der SCHULZ Systemtechnik GmbH freigegebene Cloud-Dienste zur Speicherung von Informationen der SCHULZ Systemtechnik GmbH verwendet werden.
- In Ausnahmenfällen dürfen vertrauliche Informationen für den Transport auf verschlüsselten unternehmenseigenen Wechseldatenträger (externe Festplatte) gespeichert werden. Die Verwendung von USB-Sticks ist aus Sicherheitsgründen untersagt.
- Informationen der SCHULZ Systemtechnik GmbH müssen über eine Datensicherung abgesichert werden.
- Vertrauliche Papierdokumente müssen durch Aktenvernichter oder einer Datenschutztonne gemäß min. Sicherheitsstufe P-4 entsorgt werden.
- Passwörter für Tätigkeiten für die SCHULZ Systemtechnik GmbH dürfen nicht im Browserverlauf gespeichert werden.
- Im Raum befindliche Mikrofone und Kameras von IoT-Devices (Sprachassistenten etc.) müssen bei Zugriffen oder Verarbeitung von Informationen der SCHULZ Systemtechnik GmbH ausgeschaltet sein.
- Um eine E-Mail-Kommunikation, die vertrauliche und streng vertrauliche Dateninhalte beinhaltet effektiv zu schützen, sollten E-Mails verschlüsselt übermittelt werden. Achtung: Der Betreff wird stets unverschlüsselt gesendet. Also keine vertraulichen Daten im Betreff einbauen.
- Sofern kundenspezifische Vorgaben bzgl. des Umgangs mit Informationen der Kunden der SCHULZ Systemtechnik vorhanden sind, dann sind diese Regelungen zu bevorzugen.

3 Freigegebene Dienste

3.1 IT-Dienste

Externe IT-Dienste werden ausschließlich in Absprache mit dem ISMS-Team der SCHULZ Systemtechnik GmbH evaluiert, bewertet und beschafft.

IT-Dienste	Anmerkung
Office-Programme	Keine Beschränkungen
E-Plan	Keine Beschränkungen
ERP-Software	Keine Beschränkungen
Software zur Steuerungsprogrammierung	Keine Beschränkungen
DATEV	Keine Beschränkungen
EDI-Schnittstelle	Keine Beschränkungen
VersionDog	Keine Beschränkungen
Atlassian	Keine Beschränkungen
TeamViewer	Keine Beschränkungen

3.2 Social Media:

Die SCHULZ Systemtechnik GmbH ist in verschiedenen sozialen Medien vertreten. Jeder Auftragnehmer und dessen Mitarbeiter ist im Umgang mit sozialen Medien dazu verpflichtet, unternehmensinternen

Informationen der SCHULZ Systemtechnik GmbH nicht ohne Freigabe durch die SCHULZ Systemtechnik GmbH über soziale Netzwerke preiszugeben.

3.3 Dateiaustausch

Für den Dateiaustausch mit der SCHULZ Systemtechnik GmbH müssen nachfolgende Anforderungen berücksichtigt werden.

Dateiaustausch	Anmerkung
E-Mail	E-Mails sind zu verschlüsseln.
Cloud-Dienste der SCHULZ Systemtechnik	Keine Beschränkungen.

3.4 Collaboration/Messaging Dienste

Für Informationen der SCHULZ Systemtechnik GmbH dürfen ausschließlich nachfolgende Tools zum Einsatz kommen.

Collaboration/Messaging Dienste	Anmerkung
MS Teams	Keine Beschränkungen.
Atlassian	Keine Beschränkungen.

3.5 Weitere Dienste

Die Verwendung von weiteren Diensten für die Verarbeitung oder Speicherung der Informationen der SCHULZ Systemtechnik GmbH ist untersagt. Ausnahmen dürfen ausschließlich vom ISMS-Team freigegeben werden.

4 Umgang mit Arbeitsmitteln (organisationseigenen Werten)

Alle Arbeitsmittel (wie z.B. Notebooks, PCs, mobile Festplatten, Smartphones) mit deren Hilfe vertrauliche Informationen aufbewahrt, bearbeitet weitergeleitet oder auch vernichtet werden, müssen ausreichend geschützt werden. Hierzu müssen folgende Regeln eingehalten werden:

- Schutzmechanismen die den Zutritt, Zugang oder Zugriff auf IT-Systeme, Dienste oder Informationen absichern, dürfen nicht außer Kraft gesetzt, verändert oder umgangen werden.
- Mobiles Equipment muss immer sicher oder verschlossen aufbewahrt werden.
- Es müssen Tools eingesetzt werden, die im Verlustfall vor unbefugten Zugriff schützen.
- Der Auftragnehmer stellt Sicherheitssoftware (Virenschutz, Firewall) für die Notebooks/Netbooks zur Verfügung und installiert diese.
- Die Festplatten sind nach Möglichkeit vor der Ausgabe des Geräts zu verschlüsseln (Vollverschlüsselung/ Aktive Festplattenverschlüsselung).
- Die Notebooks/Netbooks des Auftragnehmers werden vollständig durch die interne IT des Unternehmens supportet. Sie überprüft die Notebooks regelmäßig nach
  - Installierten Sicherheitsupdates
  - Patch Stand der installierten Software
  - Funktion des Virenscanners
- Die Nutzung von Unternehmensdiensten wie E-Mail, Kalender, Kontakte und Dokumenten für Informationen der SCHULZ Systemtechnik GmbH ist auf den Smartphones und Tablets des Auftragnehmers gestattet. Dabei akzeptiert der Mitarbeiter bei Einrichtung des E-Mailkontos, dass der Auftragnehmer sicherheitsrelevante Einstellungen zum Passwort/PIN und der Verschlüsselung des Smartphones bzw. Tablets prüft, dass Gerät im MDM registriert und ggf. eine Remotelöschung der Gerätedaten veranlassen kann, wenn das Gerät z.B. verloren oder gestohlen wurde.
- Bei Verwendung von Informationen der SCHULZ Systemtechnik GmbH auf den Geräten ist die Nutzung eines sogenannten „Jailbreaks“ untersagt.

- Die Nutzung von privaten Geräten (BYOD) ist für die Verwendung von Informationen der SCHULZ Systemtechnik GmbH untersagt.

5 Mobiles Arbeiten

Bei der Verwendung der Informationen der SCHULZ Systemtechnik GmbH beim mobilen Arbeiten sind folgende Punkte zu berücksichtigen:

- Bei Bedarf muss der Auftragnehmer seinen Mitarbeitern eine Sichtschutzfolie für Notebook/Monitor zur Verfügung stellen.
- Unbefugte Einsicht von Dritten verhindern (z.B. Ausrichtung des Monitors prüfen)
- Unbefugten Zugang zu Informationen verhindern (private Schlüsselregelung überdenken)
- Beim Verlassen des Arbeitsplatzes immer den Desktop sperren
- Beim Verlassen des Arbeitsplatzes keine vertraulichen Informationen auf dem Tisch liegenlassen
- Sprachassistenz-Software wie Alexa, Siri oder Google für die Dauer des mobilen Arbeitens abschalten.
- Vernichtung von vertraulichen Dokumenten nur durch Aktenvernichter ggf. im Büro vornehmen.

6 Auslandsreisen

Bei Reisen außerhalb Deutschlands kann es zu Einreisekontrollen kommen, bei denen ein Zugriff auf elektronische Geräte verlangt werden kann. Um die Geräte und die Informationen darauf zu schützen, sind folgende Verhaltensregeln zu beachten, insbesondere bei der Einreise in folgende Länder (lt. Electronic Frontier Foundation): USA, Großbritannien, Kanada, Australien.

- Bei Auslandsreisen dürfen grundsätzlich keine vertraulichen oder streng vertraulichen Informationen der SCHULZ Systemtechnik GmbH auf mobilen Datenträgern oder Endgeräten mitgeführt werden, um Schaden bei Verlust oder Spionage zu minimieren. Die Geräte sind vorher zu bereinigen.
- Notebooks sind auf Dienstreisen grundsätzlich nur mit einer Sichtschutzfolie zu verwenden und nach Möglichkeit in geschlossenen Räumen.
- Elektronische Geräte sollten im öffentlichen Raum stets im Handgepäck mitgeführt werden und nicht unbeaufsichtigt gelassen werden.
- Elektronische Geräte sollten bei längeren Wartezeiten für die Einreise im Zielland nach Möglichkeit ausgeschaltet sein, um eventuelle Fernzugriffe zu vermeiden.
- Grundsätzlich gilt: nicht verdächtig machen (Geräte nicht im Gepäck aufgeben, Informationen nicht verbergen) und respektvoll mit Beamten umgehen.
- Sollte es auf einer Dienstreise dazu kommen, dass bei der Grenzkontrolle o.ä. nach Passworten gefragt wird, sollte zuerst eine freundliche Erkundigung durch den Anwender erfolgen, ob es sich um eine Bitte oder einen Befehl handelt
  - Bei Bitte/ Wunsch: Verweigerung der Passwort-Herausgabe
  - Bei Befehl: Hinweis, dass einer Passwort-Herausgabe nicht zugestimmt wird und diese nur unter Protest erfolgt (Vorteil in ggf. Rechtsstreit)
- Sollte es zu einer detaillierteren Überprüfung der mobilen Endgeräte durch den Zoll oder anderer ausländischer Behörden kommen, bzw. sollte der Anwender den Verdacht haben, es könnten Unbefugte an seinen Endgeräten gewesen sein, ist dies umgehend dem Vorgesetzten und als Sicherheitsvorfall an den jeweiligen Leistungsanforderer der SCHULZ Systemtechnik GmbH zu melden. Ein zeitnaher Passwortwechsel für alle betroffenen Endgeräte, Datenträger und Accounts muss erfolgen.
- Sollte es auf einer Dienstreise zu einer Beschlagnahmung kommen, sollte nach Möglichkeit vorher Rücksprache mit dem jeweiligen Leistungsanforderer der SCHULZ Systemtechnik GmbH zum weiteren Vorgehen gehalten werden (Verzicht/ Abbruch der Reise).
- Vor der Ausreise sind die Geräte erneut, um ggf. gespeicherte Daten zu bereinigen.

7 Passwortrichtlinie

Passwörter sind die gebräuchlichste Form der Authentifizierung und müssen sorgfältig gehandhabt werden, um einen funktionierenden Schutz vor unbefugtem Zugriff zu gewährleisten. Ein schlecht gewähltes oder

unzureichend geschütztes Passwort gefährdet die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen. Zum Schutz der Informationen der SCHULZ Systemtechnik GmbH gelten mindestens folgende Regelungen bzgl. Passwörtern:

7.1 Vorgaben

- Passwörter müssen eine Mindestlänge von 12 Zeichen haben.
- Passwörter sollten aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Jedes Passwort muss mindestens drei dieser vier Kriterien erfüllen. Es wird empfohlen, dass Passwörter alle vier Kriterien erfüllen.
- Triviale Passwörter dürfen nicht vergeben werden z.B. das Kürzel des Benutzers darf nicht enthalten sein
- Passwörter müssen mindestens alle 180 Tage geändert werden.
- Benutzer dürfen die letzten 12 Passwörter nicht wiederverwenden.

7.2 Passwortschutz

- Benutzer müssen Passwörter vor unberechtigter Kenntnisnahme schützen.
- Initial-Passwörter müssen nach dem ersten Login geändert werden.
- Benutzer müssen vor der Eingabe ihres Passwortes sicherstellen, dass niemand das Passwort während der Eingabe beobachten kann. Umstehende sollen aufgefordert werden Diskretion zu wahren.
- Benutzer dürfen Funktionen zum Speichern von Passwörtern in Anwendungen, wie z.B. die Funktion „Autovervollständigen“ des Internet Explorers, nicht verwenden.
- Passwörter dürfen nicht im Klartext gespeichert werden.
- Passwörter dürfen nicht an Unberechtigte oder zu Delegationszwecken weitergegeben werden.
- Wenn der Benutzer Grund zur Annahme hat, dass ein Dritter sein Passwort kennt, muss der Benutzer es unverzüglich ändern.
- Wenn ein Benutzer Grund zu der Annahme hat, dass sein Passwort missbraucht wurde, muss er dies als Sicherheitsvorfall melden.
- Dienstlich verwendete Passwörter dürfen nicht privat genutzt werden.
- Kein Notieren von Anmeldeinformationen oder unverschlüsselte Speicherung

8 Clear Screen Policy

Folgende Sicherheitsmaßnahmen sind einzuhalten:

- Bei Verlassen des Arbeitsplatzes muss der Zugang zu Notebooks und lokalen Computern gesperrt werden (Windows-Taste + L oder Abmeldung).
- Die Geräte werden bei der Einrichtung von der IT des Auftragnehmers so voreingestellt, dass nach 15 Minuten die automatische Bildschirmsperre aktiviert wird. Diese Voreinstellung darf nicht deaktiviert werden.
- Bei der Anzeige vertraulicher Informationen auf dem Bildschirm sollte sich der Benutzer versichern, dass kein unbefugter Dritter Einsicht auf den Bildschirm hat.
- Beim Arbeiten mit vertraulichen Informationen der SCHULZ Systemtechnik GmbH von unterwegs soll eine Bildschirmsichtschutzfolie verwendet werden.

9 Clear Desk Policy

Folgende Sicherheitsmaßnahmen sind einzuhalten:

- Jeder Mitarbeiter muss bei Abwesenheit seine vertraulichen Unterlagen der SCHULZ Systemtechnik GmbH verschließen.
- Vertrauliche Informationen der SCHULZ Systemtechnik GmbH sollen für unberechtigte Dritte nicht einsehbar sein

10 Sicherheitsvorfälle

Die Mithilfe jedes einzelnen Mitarbeiters des Auftragnehmers ist unverzichtbar. Hierzu zählt insbesondere aufmerksam auf Ereignisse zu achten, die möglicherweise eine Beeinträchtigung der Informationssicherheit oder Datenschutzverletzung bedeuten können. Jede nicht erfolgte Meldung birgt Risiken für die Betroffenen und das Unternehmen.

10.1 Beispiele für Sicherheitsvorfälle

- Diebstahl oder Verlust eines Rechners
- Diebstahl oder Verlust eines Datenträgers mit sensiblen Daten
- Rechner wird mit Verschlüsselungstrojaner infiziert
- plötzliche Veränderungen an vertraulichen Dateien
- ungewöhnlichen E-Mail- und Netzwerk-Aktivität
- nicht autorisierte Verwendung von Ressourcen
- Informationsabfluss
- physikalische Beschädigung der mobilen Endgeräte
- Hardwarewartungsfehler
- Softwarewartungsfehler
- Netzwerk Fehler
- Planungsfehler
- Systemausfall
- selbst verursachte Sicherheitsvorfälle
- Hackerangriff auf die IT-Systeme und Abzug von Daten
- versehentlicher elektronischer Versand einer unverschlüsselten Liste mit Daten
- an einen unrechtmäßigen Empfänger
- fehlerhafte Verteilung von Zugriffsberechtigungen auf Laufwerke
- Verwendung von geschäftlichen Daten für private Zwecke
- Verlust oder Diebstahl des Laptops oder eines anderen Datenträgers, wenn die Daten darauf nicht oder nicht ausreichend verschlüsselt sind
- Verlust oder Diebstahl einer Videokamera und des Aufzeichnungsmaterials
- Veröffentlichungen von Daten im Internet aufgrund eines technischen Fehlers
- …

10.2 Melden von Sicherheitsvorfällen

Der Auftragnehmer muss Informationssicherheitsvorfälle und Probleme in Bezug auf die SCHULZ Systemtechnik GmbH unverzüglich über einen der eingerichteten Kommunikationskanäle melden:

- E-Mail an helpdesk@schulz.st

Vorab sind Auffälligkeiten und Beweise zu sichern die als Nachweis bzw. zur Aufklärung des Vorfalls dienen können.

Wann liegt eine akute Bedrohung vor?

- Bei Verlust der Kontrolle über die Daten

Gemeldet werden müssen alle Arten von Sicherheitsvorfällen:

- tatsächlich eingetreten
- Versuch
- Verdacht
- Vorsätzlich

Die schriftliche Meldung sollte folgende Angaben enthalten:

- Datum des Vorfalls
- Uhrzeit des Vorfalls
- Beschreibung des Vorfalls oder der Beobachtung und ggf. gesicherte Nachweise als Anhang.

10.3 Sammeln von Beweismaterial

Bei Sicherheitsvorfällen mit einem Schaden, bei denen die Polizei oder eine andere Behörde (zum Beispiel der Datenschutz) tätig wird, muss der Vorfall umgehend an die IT und das ISMS-Team der SCHULZ Systemtechnik GmbH gemeldet werden, um das Beweismaterial für die Ermittlungen ohne Verluste bereit zu stellen und die Sicherheit der Mitarbeiter nicht zu gefährden.

Notwendige Beweise können sein:

- Archivierungen
- LogFiles
- Netzwerkverbindungen
- Forensisches Beweismaterial
- Hardcopies
- HDD
- Screenshots
- Das Offlinenehmen von laufenden Servern
- Sonstiges

Falls es zu einem Vorfall kommt, bitte immer als erstes die IT informieren und den Zugriff auf das Beweismaterial sicherstellen!

11 Sanktionen

Bei Zuwiderhandlung gegen das Regelwerk zur Informationssicherheit behält sich die Geschäftsleitung der SCHULZ Systemtechnik GmbH vor rechtliche Schritte einzuleiten.