Richtlinie zur Informationssicherheit im Zusammenhang mit Lieferbeziehungen

– kurz: IT-Sicherheitsrichtlinie Lieferanten –

Inhalt

1. Geltungsbereich

(1.1.) Die Richtlinie gilt für alle Mitarbeiter der Schütz Gruppe und deren Lieferanten, die an IT-Dienstleistungen beteiligt sind. IT-Dienstleistungen umfassen alle Ausprägungen des Bezugs von IT. Dazu zählen unter anderem die Breitstellung von IT-Systemen, Projekte/Gewerke oder Personalgestellung. Darin inbegriffen ist die Auslagerung/Outsourcing oder sonstiger Fremdbezug von IT-Dienstleistungen. Dazu gehören neben Mitarbeitern der IT und des Einkaufs auch die für die Beschaffung oder IT verantwortlichen Mitarbeiter aller Schütz-Fachbereiche, die der Lieferanten sowie deren Unterlieferanten. Die Geheimhaltungsklasse wird in im „Non-disclosure agreement“ (NDA) definiert.

2. Ziel und Gegenstand der Richtlinie

(2.1.) Das Ziel dieser Richtlinie ist der Schutz der für Lieferanten zugänglichen Unternehmenswerte der Schütz Gruppe. Dabei sollen die Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) der Informationssicherheit gewahrt werden, um Sicherheitsrisiken zu verhindern.

(2.2.) In der Richtlinie zur Informationssicherheit im Zusammenhang mit Lieferbeziehungen werden wesentliche Inhalte bezüglich der Informationssicherheit und des Datenschutzes geregelt, die sich ergeben, wenn Schütz in Zusammenarbeit mit Lieferanten IT-Beschaffungen durchführt. Diese Richtlinie stellt eine Ergänzung der allgemeinen betrieblichen Bestimmungen zur Informationssicherheit und dem Datenschutz dar und erweitert den Geltungsbereich ausdrücklich um die Firmen, die als Lieferanten für die Schütz Gruppe fungieren. Die Richtlinie ersetzt nicht den NDA.

(2.3.) Damit eine Beschaffung zustande kommt, sollte diese Richtlinie vor dem Abschluss eines Geschäfts dem Lieferanten zur Verfügung gestellt und geprüft werden. Eine schriftliche Bestätigung des Lieferanten über den Erhalt des Dokuments und der Zustimmung zu den Inhalten ist in jedem Fall erforderlich.

(2.4.) Der Lieferant verpflichtet sich, im Rahmen des nach dem jeweiligen Stand der Technik, alle Informationen und Daten, gemäß den genannten Informationssicherheitsmaßnahmen von Schütz, sofort und wirksam zu schützen.

3. Informationssicherheitsmaßnahmen

(3.0.) In den nachfolgenden Unterkapiteln werden die geltenden Regeln für Lieferanten/Dienstleister definiert. Die Verbotshinweise zeigen ein Verhalten auf, welches untersagt ist. Die Warnhinweise dienen zur Information und Sensibilisierung. Die Gebotshinweise legen Vorgaben fest.

3.1. Verbotshinweise 

(3.1.1.) Zugriffe auf mobile Wechseldatenträger (USB-Stick, Disketten, SD-Karten, CD/DVD, usw.) sind zu vermeiden. Die Verwendung von Schütz-gelieferten Datenträgern ist erlaubt. USB-Schnittstellen sind standardmäßig systemseitig gesperrt. Sollte eine Freigabe für die USB-Benutzung notwendig sein, dann muss der Schütz Mitarbeiter diese Nutzung über das interne HelpDesk-System beantragen. Verwenden Sie für externe Datenübertragungen https://share.schuetz.net/. Der Versand von vertraulichen/streng vertraulichen Daten ist nur verschlüsselt über „share.schuetz.net“ erlaubt.

(3.1.2.) Alle Benutzerkonten sind systemseitig mit einem Kennwort versehen. Benutzer müssen ihre Kennwörter alle 90 Tage ändern. Dieser Kennwortverfall darf nicht deaktiviert werden. Ausgenommen vom Kennwortverfall sind bestimmte System-, Kommunikation-, Service-, Sammel- oder Produktionsbenutzer. Kennwörter dürfen nicht in Klartext auf den Komponenten gespeichert oder handschriftlich festgehalten werden.

(3.1.3.) Jegliche Netzwerkgeräte wie Switche, Router, Access Points, Firewalls, usw. werden ausnahmslos von Schütz gestellt. Netzwerkdienste wie DNS, DHCP, WINS, PXE oder ähnliche dürfen im internen Schütz Netzwerk nur nach Absprache mit der IT gestartet oder betrieben werden. In begründeten Ausnahmen kann der Einsatz von Netzwerkgeräten, die der Lieferant betreibt, von der IT geprüft und genehmigt werden.

(3.1.4.) Die Offenlegung oder das zur Verfügung stellen von Daten oder Informationen gegenüber Dritter (z. B. Familienangehörigen) ist nicht gestattet. Der Zugriff oder Zugang (z. B. im Home-Office) durch Dritte ist ebenfalls nicht gestattet.

(3.1.5.) Der reguläre Druck im Schütz-Netzwerk auf den Etagendrucker ist nicht gestattet. Beim Ausdrucken ist der „vertrauliche“ Druck zu verwenden. Unbefugtes Fotografieren ist nicht erlaubt.

(3.1.6.) Von einer unverschlüsselten Kommunikation ist abzusehen. Eine Datenverschlüsselung ist immer dann zwingend vorzusehen, wenn über unsichere Medien (z. B. Internet) auf schutzwürdige Daten oder Anwendungen zugegriffen werden. Bei der Verschlüsselung sind keine unsichere, schwache oder bereits kompromittierte Verschlüsselungsalgorithmen und Schlüssellängen zu verwenden. Es ist jeweils der stärkste Verschlüsselungsalgorithmus und die sicherste Schlüssellänge einzurichten. Sollte dies nicht möglich sein, so kontaktieren sie die IT Security.

(3.1.7.) Die vom Lieferanten eingesetzte Software oder Hardware ist mittels technischer oder organisatorischer Mittel zu warten bzw. upzudaten. Ausnahmen werden gesondert durch die IT Security bewertet.

(3.1.8.) Bei Arbeiten an neuen Komponenten oder bereits betriebenen Komponenten werden keine unsichere Konfiguration hinterlassen. Die Konfiguration ist nach dem Stand der Technik vorzunehmen.

(3.1.9.) Eigenes Equipment darf nicht eigenständig eingesetzt werden. Sollte es notwendig sein mitgebrachtes Equipment einzusetzen, bedarf dies der Zustimmung der IT.

3.2. Warnhinweise

(3.2.1.) Zu Monitoring- und Compliance-Zwecken werden alle Zugriffe protokolliert. Einwahl-, Login- und Logout- sowie Zugriffsdaten (Benutzername, Datum, Uhrzeit und An-/Abmeldung) werden zentral protokolliert**.** Schütz hält sich vor sämtliche anfallende Protokolldaten gemäß der gültigen, internen Betriebsvereinbarung zu speichern. Dazu gehören Internetzugriff, Remote Access Zugriffe, An- und Abmeldungen, E-Mail-Transfers, usw.

(3.2.2.) Verbindungen zu Systemen, angemeldete Benutzer und ausgeführte Tätigkeiten bzw. Transaktionen werden im Rahmen einer ständigen, automatisierten Überwachung gespeichert. Auswertung erfolgt unter Wahrung des Datenschutzes. Für Arbeiten im Werksgelände gelten gesonderte Regelungen.

(3.2.3.) Der Fernzugriff (Remote Access) kann nicht frei gewählt werden. Folgende Arten von Fernzugriffen werden von Schütz angeboten:

- WatchGuard Mobile VPN per SSL für den individuellen Fernzugriff von einem Rechner außerhalb des internen Netzwerkes.
- Für den spontanen Support bspw. zur Fernsteuerung oder -wartung von Rechnern steht Cisco Webex oder TeamViewer zur Verfügung.

(3.2.4.) Der beauftragte Dienstleister kann sich jederzeit mit einem Personalausweis oder einem durch den Lieferanten signierten und ausgestelltem Dokument für die Beauftragung ausweisen. Der Personalausweis oder das signierte Dokument ist vor dem Erhalt des Besucherausweises eigenständig vorzuweisen sowie auf Verlangen vorzuzeigen. Sollte diese Richtlinie vorsätzlich oder fahrlässig missachtet werden kann dies ein Hausverbot zur Folge haben.

(3.2.5.) Besucher müssen während ihres Aufenthaltes beaufsichtigt werden und erhalten nur Zugang zu den für ihren Aufenthalt erforderlichen Bereichen. Mit dem Kapitel „Verhalten im Notfall“ werden die Sicherheitsanforderungen im Notfall unterrichtet.

(3.2.6.) Das Personal stellt sicher, dass Dritte nur gemäß dem Need-to-Know-Prinzip für Arbeiten/Aktivitäten innerhalb sensibler Bereiche informiert sind. Sie erhalten so viele Informationen wie es für die Ausübung der jeweiligen Tätigkeit erforderlich ist.

(3.2.7.) Der Zugriff aus dem Schütz Netzwerk auf das Internet kann auch über das Gäste-Netz erfolgen. Der dazu notwendige Antrag kann durch Schütz Mitarbeiter über die Besucherverwaltung oder direkt an der Zentrale erfolgen.

(3.2.8.) Es muss sichergestellt sein, dass ausschließlich nach Stand der Technik gesicherte Geräte und Komponenten zur Wartung und Konfiguration genutzt werden.

(3.2.9.) Gesetzliche und regulatorische Anforderungen, einschließlich Datenschutz, geistigem Eigentum und Copyright werden eingehalten. Bei Supportanfragen, Störungen, Problemen oder Vorfällen ist das Schütz IT HelpDesk zu benachrichtigen.

(3.2.10.) Für eine vorausschauende Planung und Gestaltung von IT-Komponenten. Sind diese vor der Beschaffung bzw. Beauftragung mit der IT abzuklären. Damit stellt man unter anderem eine Kompatibilität sicher.

3.3. Gebotshinweise

(3.3.1.) Die an der Beschaffung beteiligten IT-Ansprechpartner des Lieferanten sind im Zuge der Anbahnung von Aufträgen zu benennen: IT-Fachverantwortlicher, IT-Vertrieb, IT-Security/Informationssicherheitsbeauftragter. Unter dem Kapitel „Verpflichtung und Ansprechpartner“ werden die genannten Rollen namentlich eingetragen. Sollten die genannten Rollen nicht gegeben sein, so benennen Sie die Verantwortlichen.

(3.3.2.) Angebote, Auftragsbestätigungen, Rechnungen und andere Dokumente mit IT-Komponenten sind ausführlich auszuweisen. Dazu gehören die eindeutigen Angaben zu Hersteller, Modell, Edition, Version, Lizenz-Metrik, Generation, Anzahl, Währung, Einzelkosten, usw. Bei Softwarekomponenten sind Lizenzen und Software-Wartung zu trennen. Bei Projektpreisen oder rabattierten Preisen sind – wenn möglich – trotzdem die Einzelpreise der Lieferungen oder Leistungen auszuweisen. Die Leistungen der Wartung oder des Supports sind einzeln aufzuführen.

(3.3.3.) Wenn möglich stellt Schütz die Client- oder Server-Hardware inklusive der initialen Betriebssystem-Installation durch einen automatisierten und standardisierten Prozess. Windows Rechner kommen in die Domäne und erhalten Virenschutz. Der Zugriff von fremden Netzwerk-Komponenten auf interne Netzwerk-Ressourcen kann nur nach expliziter Freigabe der Schütz IT erfolgen.

(3.3.4.) Jegliche auf Clients oder Servern eingesetzte Software muss der IT gemeldet werden. Je nach Nutzungsgrad wird die zu verwendende Software zentral durch Schütz paketiert. Dies ist mit der Schütz IT abzustimmen.

(3.3.5.) Alle digitalen Benutzer für externe Mitarbeiter sind von dem zuständigen Schütz Mitarbeiter über das Schütz-interne Helpdesk-System zu beantragen. Die Genehmigung von administrativen Berechtigungen (Windows Administrator, Linux root oder Microsoft SQL sa) ist nur in begründeten Einzel- und Ausnahmefällen gestattet, bspw. für Installationen oder Inbetriebnahmen oder ein vergleichbares Szenario. Zugriffsberechtigungen werden restriktiv vergeben.

(3.3.6.) Der tägliche Betrieb der Systeme ist stets ohne administrative Rechte sicherzustellen. Computer und mobile Geräte sind vor unberechtigter Nutzung durch Tastensperre oder ähnlichem, wie z. B. Passwortschutz zu schützen, sobald diese nicht in Gebrauch sind. Alle Lieferanten, Besucher und sonstige Dritte müssen den ausgehändigten Besucherausweis gut sichtbar tragen.

(3.3.7.) Die Authentifikation von Systemen oder Lösungen sollte an das zentrale Microsoft Active Directory der Schütz Gruppe angebunden werden. Dezentrale Benutzerverwaltungen sind zu vermeiden und mit der Schütz IT abzustimmen.

(3.3.8.) Jegliche Zugangsdaten (Benutzernamen, Kennwörter, Codes, PINs, usw.) sind vertraulich zu behandeln. Darunter fallen ebenso physikalische Schlüssel oder Zutritts-Chips (Legic, RFID, usw.) Es ist die Clean-Desk-Regel anzuwenden. Bei Beendigung der Beauftragung ist die Abgabe von physischen Zutrittsmitteln (z. B. Chip, Schlüssel, usw.) zu vollziehen.

(3.3.9.) Der Lieferant ist zur Einhaltung aller datenschutzrechtlichen Bestimmungen in der jeweils geltenden Fassung verpflichtet und muss diese beachten. Der Lieferant hat alle Mitarbeiter nach den jeweils gültigen datenschutzrechtlichen Bestimmungen zu

belehren und auf das Datengeheimnis zu verpflichten. Diese Erklärungen sind dem Datenschutzbeauftragten von Schütz auf Verlangen vorzulegen.

3.4. Verhalten im Notfall

Wenn Sie einen Verdacht auf eine Vireninfektion oder Ähnliches haben, stellen Sie Ihre Arbeit ein und melden Sie Ihren Verdacht dem IT-Helpdesk. Führen Sie keine Maßnahmen ohne Anweisung der IT durch. Prägen Sie sich alle Auffälligkeiten gut ein und dokumentieren Sie diese. Sollte es sich um einen Datenschutzverstoß handeln, kontaktieren Sie zusätzlich den Datenschutzbeauftragten.

1.) Bewahren Sie Ruhe! Unkoordinierte Handlungen können wertvolle Beweise vernichten.

2.) Trennen Sie das Gerät vom Netzwerk. Dies impliziert das kabelgebundene als auch das drahtlose Netzwerk. Die IT wird Sie bei Problemen unterstützen.

3.) Fahren Sie das Gerät nicht herunter und schalten Sie es nicht aus! Sie könnten dadurch wertvolle flüchtige Analysedaten vernichten. Ein IT-Mitarbeiter wird diese Daten sichern.

4.) Das Gerät kann nach der Sicherung ausgeschaltet werden. Das Gerät wird von der IT zur weiteren Analyse und Sicherung eingesammelt.

5.) Das Gerät wird neuinstalliert und benötigte Programme und Daten werden wiederhergestellt.

IT-Notfallkontakte:

IT Helpdesk:

Hotline: +49 2626 77955
E-Mail: helpdesk@schuetz.net
Portal: helpdesk.schuetz.net

Servicezeiten: Montag - Freitag 07:00 Uhr - 18:00 Uhr
IT-Rufbereitschaft Außerhalb dieser Servicezeiten: +49 2626 77-1331

IT-Security Abteilung - E-Mail: itsecurity@schuetz.net

Leiter der IT Security Abteilung Sven Westenberg:
Büro: +49 2626 77-419 / +49 2626 77-18419
Mobil: +49 1752 286592
E-Mail: sven.westenberg@schuetz.net

Pförtner (Selters):
Kontakt: +49 2626 77-260

Datenschutzbeauftragter Christian Baier:
Büro: +49 2626 77-740
E-Mail: datenschutz@schuetz.net

4. Verpflichtung und Ansprechpartner

4.1. Verpflichtung zur „Richtlinie zur Informationssicherheit im Zusammenhang mit Lieferbeziehungen “

Der Lieferant hat diese Richtlinie gelesen, verstanden und ist mit den Inhalten und seinen Pflichten einverstanden. Zudem stellt er sicher, dass seine beauftragten Mitarbeiter sowie Subdienstleister zu der Richtlinie unterwiesen worden sind. Das Verhalten im Notfall wurde hiermit instruiert.

_____

(Version dieser Richtlinie)

_____

(Firma)

_____

(Straße, Postleizahl, Ort)

_____

(Titel, Nachname, Vorname)

_____

(Ort, Datum, Unterschrift)

4.2. Ansprechpartner der oben genannten Firma:

(siehe Punkt (3.3.1.))

_____

_____

(Nachname, Vorname, Rolle) (E-Mail-Adresse, Telefonnummer)

_____

_____

(Nachname, Vorname, Rolle) (E-Mail-Adresse, Telefonnummer)

_____

_____

(Nachname, Vorname, Rolle) (E-Mail-Adresse, Telefonnummer)

_____

_____

(Nachname, Vorname, Rolle) (E-Mail-Adresse, Telefonnummer)

5. Änderungsübersichtstabelle

Nr.	Datum	Version	Name/Abt.	Änderungsbeschreibung
1	27.04.2022	V1.0	Wika von Czarnowski, David / IT-Security	Initiale Erstellung des Dokuments
2	02.05.2022	V1.0	Wika von Czarnowski, David / IT-Security	Finalisierung nach der internen Klärung
3	22.02.2023	V1.0	Sven Westenberg / IT-Security	Kurzbezeichnung, Informationsklassifizierung
4	18.09.2023	V2.1	Steven Beck; Sven Westenberg / IT-Security	Jährliche Überarbeitung mit redaktionellen Änderungen. NAC Passage hinzugefügt.