Richtline für Informationssicherheit (IT-Sicherheit und Datenschutz) der Kurt Müller GmbH:

1. Gültigkeit

Als Mitarbeitende der Kurt Müller GmbH (nachfolgend Unternehmen) regelt diese IT-Sicherheitsrichtlinie vorrangig alle für Sie relevanten IT-Sicherheits- und Datenschutz-Themen. Weitere Vereinbarungen (z.B. Arbeitsvertrag) sind hiervon nicht betroffen und zusätzlich gültig.

Anmerkung:
Im Folgenden wird an manchen Stellen auf „unberechtigte Dritte“ verwiesen. Organisationen und Personen, mit denen gültige Verträge vorliegen, zählen nicht zu den unberechtigten Dritten.

2. Allgemeine Bestimmungen

Geltende Gesetze
Jeder Mitarbeiter ist in seinem Zuständigkeitsbereich für die Einhaltung der geltenden Regelungen, Anweisungen sowie Gesetze zuständig.
Die Verwendung von Unternehmens-Ressourcen ist nur in einer gesetzlich zulässigen und der Arbeitsumgebung angemessenen Weise und nicht für moralisch verwerfliche Zwecke erlaubt.

3. Urheberrecht

Bitte beachten Sie das Urheberrecht. **Geben Sie keine Informationen als Ihre eigenen aus, für die Sie nicht das Urheberrecht besitzen.**

4. Verstöße

Verstöße gegen die im Unternehmen geltenden Richtlinien und Vorgaben (inkl. dieser Richtlinie) können arbeitsrechtliche sowie strafrechtliche Konsequenzen haben.

5. Allgemeine Vertraulichkeitsklausel

Weitergabe von Unternehmenswerten
Eine Weitergabe von Unternehmenswerten (Informationen, Daten, Lizenzen, Firmeneigentum o.ä.) an unberechtigte Dritte ist ohne ausdrückliche Freigabe durch die Geschäftsführung oder einen Prokuristen weder digital noch in Papier oder durch mündliche Auskunft erlaubt.
Stellen Sie auch die Gewährleistung der Vertraulichkeit in Kundenprojekten gegenüber unberechtigten Dritten sicher. Im Zweifelsfall fragen Sie Ihre zuständige Führungskraft.

Datenschutz
Sollten Sie in Ihrem Aufgabenbereich mit personenbezogenen Daten von Mitarbeitern oder anderen Firmen oder Privatpersonen in Kontakt kommen, dann gehen Sie mit diesen Informationen vertraulich um.
Vertraulichkeit und Geheimhaltung in Kundenprojekten
Zusätzlich sind die jeweils gültigen Geheimhaltungserklärungen der Kunden anzuwenden.

6. Datenschutz

Aufgrund Ihrer Aufgabenstellung verpflichten Sie sich auf die Wahrung des Datengeheimnisses nach der Europäischen Datenschutzgrundverordnung bzw. dem Bundesdatenschutzgesetz (BDSG)
Es ist Ihnen nach dieser Vorschrift untersagt, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Wir verweisen auf die separate
Verpflichtungserklärung zur Wahrung des Datengeheimnisses gemäß § 53 Bundesdatenschutzgesetz (BDSG-neu), des Fernmeldegeheimnisses gemäß § 88 Telekommunikationsgesetz (TKG) und zur Wahrung von Geschäftsgeheimnissen
Diese Verpflichtung besteht auch nach Beendigung Ihrer Tätigkeit fort.
Verstöße gegen das Datengeheimnis können mit Freiheits- oder Geldstrafe geahndet werden. In der Verletzung des Datengeheimnisses kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Schweigepflichten liegen.

7. Digitale Informationen

Sichern von Daten
Um die Verfügbarkeit von Daten zu gewährleisten, ist es zwingend, dass die Daten immer auf den Serverlaufwerken gesichert werden.
Vertrauliche Daten dürfen nur mit Zustimmung Ihrer Führungskraft lokal abgelegt werden. Klären Sie für diesen Fall mit den IT-Verantwortlichen, dass Ihr Laptop über eine verschlüsselte Festplatte verfügt. Löschen Sie nach Rückkehr ins Unternehmen umgehend die Daten von der lokalen Platte und sichern Sie diese auf den entsprechenden Serverlaufwerken.

Firmendaten auf Privatgeräten
Das Speichern von Firmendaten auf privaten Rechnern ist nicht erlaubt.

8. Firmenhard- und -software / Daten

Für die IT-Ausstattung, die Ihnen vom Unternehmen für die Ausübung Ihrer beruflichen Tätigkeit übergeben wurde, sind Sie verantwortlich.

Rechner, Laptops und Ipads
Die private Nutzung der Rechner, Laptops und Ipads ist mit folgenden Einschränkungen erlaubt: Nutzen Sie die Geräte nur für legale Zwecke.

Eine Verwendung für Nebentätigkeiten ist nicht gestattet.
Eine Mitnahme der Geräte auf private Reisen ist nur nach Zustimmung Ihrer Führungskraft gestattet.
Evtl. entstandene Kosten durch die private Nutzung müssen privat bezahlt werden (z.B. kostenpflichtige Einwahl in ein WLAN).
Die eigenständige Installation von Software ist nur für betriebliche Zwecke und nach Rücksprache mit Ihrer Führungskraft / IT-Verantwortlichen erlaubt.
Stellen Sie bitte sicher, dass die Ausstattung außerhalb des Arbeitsortes immer sicher aufbewahrt wird und nicht für unberechtigte Dritte zugänglich ist.

9. Mobilgeräte

Die private Verwendung der Ihnen überlassenen Mobilgeräte ist gestattet.
Bei kostenpflichtigen Diensten ist die private Verwendung im Rahmen der Flatrate für Telefonie und Internet erlaubt.
Kostenpflichtige Dienste (z.B. bei privater Nutzung im Ausland) sind vorher abzustimmen.
Verwenden Sie die Geräte nicht für illegale Zwecke.
Die Installation von kostenpflichtigen Apps für private Zwecke können Sie über Ihre privaten Kontodaten durchführen.
Die Nutzung Ihrerseits setzt voraus, dass Sie sich damit einverstanden erklären, dass die Protokolle (Telefonie, Internet) ausgewertet werden dürfen. Nutzen Sie das Gerät nicht privat, wenn Sie damit nicht einverstanden sind.

10. Private Daten

Die Nutzung privater Daten auf Firmenrechnern (nur Endgeräte, keine Serverlaufwerke) ist mit folgenden Einschränkungen erlaubt:
Die privaten Daten dürfen keine Urheberrechtsverletzung darstellen.
Speichern Sie keine illegalen Daten.
Die Firma übernimmt keine Haftung für die Sicherheit und Verfügbarkeit der Daten.
Die Speicherung erfolgt auf eigenes Risiko.
Auf Anweisung sind die Daten wieder zu löschen.

11. Private Hard- und Software

Private Laptops

Die Nutzung privater Laptops als Unternehmensarbeitsgerät ist nur in Abstimmung mit der Geschäftsleitung bei begründeten Fällen erlaubt
Verwenden Sie eine eigene Virtuelle Umgebung für den Unternehmenszweck und trennen Sie damit die geschäftliche und private Nutzung.
Alternativ kann die Trennung durch einen eigenen Benutzer auf dem Gerät erfolgen.
Es muss sichergestellt werden, dass unberechtigte Dritte keinen Zugriff auf Unternehmensdaten und Unternehmenslizenzen erhalten.

Die Festplatte des Geräts muss verschlüsselt sein.
Stellen Sicher, dass das Gerät einen Schutz gegen Viren und Schadprogramme enthält, sofern dies dem Stand der Technik entspricht.
Bei dem Gerät darf es sich nicht um ein Familiengerät handeln, das von mehreren verschiedenen Personen genutzt wird.

Private Tablets / Mobiltelefone
Die Verwendung ist erlaubt zur:
E-Mail-Synchronisation
Ein Passwortschutz muss auf dem Gerät eingerichtet sein, wenn es für betriebliche Daten verwendet wird.
Bei dem verwendeten Gerät darf es sich nicht um ein Gerät handeln, das von mehreren Personen verwendet wird (z.B. Tablet, das von der ganzen Familie genutzt wird).
Nutzen Sie private Geräte während der Arbeitszeit nur in verhältnismäßigem Umfang (z.B. für ein kurzes Telefonat, kein permanentes Chatten)
Private Kameras / bzw. Kameras privater Mobiltelefone
Die Verwendung ist erlaubt.
Die Übertragung der Fotos sollte nicht über einen Anschluß an den Firmenrechner, sondern per E-Mail erfolgen.
Private Speichermedien
Die Verwendung privater Speichermedien ist nur nach Rücksprache mit Ihrer Führungskraft erlaubt.
Firmendevices werden bei Bedarf ausgegeben.

12. Datenaustausch

mit externen Parteien (zur Projektabwicklung)
Datenaustausch erfolgt per E-Mail. Zu beachten ist, dass vertrauliche Informationen verschlüsselt zu versenden sind!
Datenaustausch per Speichermedium – auch hier sind vertrauliche Daten verschlüsselt abzulegen. Datenaustausch durch Cloudnutzung kann auf Kundenanforderung (nur Projektdaten) erfolgen.

13. Zutritt / Zugang

Für Ihre persönlichen Zutritts- und Zugangskennungen sind Sie verantwortlich. Gehen Sie daher bitte sorgsam damit um. Übertragen Sie keine Zutrittskennungen bzw. Schlüssel / Ausweise unautorisiert an Dritte. Geben Sie Zugangskennungen nicht an Dritte weiter.
Nicht mehr benötigte Zugänge
Lassen Sie bitte elektronische oder physikalische Zugangs- oder Zutrittsberechtigungen umgehend deaktivieren, wenn diese nicht mehr benötigt werden.

14. Pass-/ Kennwörter

Geben Sie Ihr Pass-/Kennwort nie an Dritte weiter!
Es gilt die folgende Kennwortrichtlinie:
Kennwort muss Komplexitätsvoraussetzungen entsprechen

Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen.
Das Kennwort muss mindestens acht Zeichen lang sein.
Das Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten:

- Großbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)
- Zahlen zur Basis 10 (0 bis 9)
- Nicht alphabetische Zeichen (zum Beispiel !, $, #, %)

15. E-Mail

Private Nutzung
Die private Nutzung des betrieblichen E-Mail Accounts ist nicht erlaubt.

Abwesenheit
Bitte aktivieren Sie den Abwesenheitsagenten bei geplanter Abwesenheit.
Die Weiterleitung von E-Mails durch den Administrator kann bei Abwesenheit eines Mitarbeiters durch die Anordnung der Geschäftsleitung erfolgen.
Falls möglich, wird der Arbeitnehmer kontaktiert, um die Mails persönlich weiterzuleiten.

16. Internet

Allgemein
Die Internetnutzung im Unternehmensnetzwerk wird protokolliert. Internetprotokolle können ausgewertet werden.
Das Aufrufen von Web-Seiten mit pornographischen, gewaltverherrlichenden, rassistischen, unsittlichen oder in Konflikt mit dem Gesetz stehenden Inhalten sowie die Verbreitung solcher Inhalte im Firmennetzwerk ist streng verboten.

17. Private Internet-Nutzung

Das Unternehmen erlaubt Ihnen eine private Nutzung des Internets. Die Nutzung Ihrerseits setzt voraus, dass Sie sich damit einverstanden erklären, dass die Internetprotokolle ausgewertet werden dürfen. Nutzen Sie das Internet nicht privat, wenn Sie damit nicht einverstanden sind.
Die gewährte private Nutzung ist eine unverbindliche, jederzeit widerrufbare Vergünstigung, auf die kein Anspruch besteht. Das Unternehmen übernimmt keine Gewähr für die Verfügbarkeit der privaten Nutzung.

Dienstliche Belange haben stets Vorrang. Sofern aus dienstlichen Gründen erforderlich, kann die private Nutzung zeitweise unterbrochen werden. Die Haftung unseres Unternehmens im Zusammenhang mit der kostenfrei gewährten Privatnutzung ist ausgeschlossen, soweit nicht Vorsatz oder grobe Fahrlässigkeit durch das Unternehmen nach § 521 BGB vorliegen.
Das Angebot der privaten Nutzung zieht keinen Verfügbarkeitsanspruch an den betrieblichen Internetdienst nach sich.
Nutzen Sie das betriebliche Internet nicht für das Abrufen von unmittelbar kostenpflichtigen Informationen oder Dienstleistungen für den Privatgebrauch (z. B. unmittelbar kostenpflichtige Informationsdienste). Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden (z. B. Powerseller bei ebay).
Der Download von großen Dateien (Videos, Installationspakete etc.) ist ausschließlich für betriebliche Zwecke erlaubt.
Nutzen Sie das betriebliche Internet
Nicht für private Downloads
Nicht zu illegalen Zwecken
Beachten Sie, dass die Verhältnismäßigkeit der privaten Nutzung erhalten bleibt.

18. Netzwerk

Im Unternehmen
Nehmen Sie keine Änderungen an den Datennetzen oder den zugrunde liegenden technischen Einrichtungen vor, es sei denn, Sie sind dazu ausdrücklich befugt. Insbesondere ist es nicht zulässig, unerlaubt Zugänge zu den Netzen (z. B. Einwahlzugänge, Anbindungen an Fremdnetze) zu schaffen. Derartige Zugänge werden ausschließlich durch die IT bereitgestellt.
Schaffen Sie keine „Brücken“ ins interne Netzwerk (z. B. durch das Herstellen einer zweiten Netzwerkverbindung ins Internet über WLAN oder eine zweite Netzwerkkarte).
Nutzen Sie keine privaten IT-Geräte (BYOD) im Unternehmensnetzwerk. Dies gilt auch für mobiles Arbeiten oder Homeoffice.

Externe Verbindungen (z.B. Teamviewer, Teams)
Zu Supportzwecken oder im Rahmen von Online-Meetings, kann es notwendig sein, dass Sie eine Verbindung von Ihrem Arbeitsplatzrechner herstellen. Beachten Sie folgende Vorgaben, wenn Sie eine solche Verbindung aufbauen:
Mitarbeitende, die diese Verbindung initiieren, bzw. den Bildschirm teilen, sind verantwortlich für die dem externen Partner gegenüber sichtbaren Daten und Anwendungen.
Stellen Sie sicher, dass keine sicherheitskritischen Daten und Informationen während der geöffneten Sitzung zur Verfügung stehen bzw. von Ihnen per Datentransfer übertragen werden.
Ist ein Datentransfer z. B. aus Supportgründen notwendig, müssen Sie sicherstellen, dass in diesem Fall der externe Partner mit den erhaltenen Daten entsprechend sorgfältig umgeht und zu diesen keine weiteren fremden Dritten Zugriff erlangen.

Hier ist im Vorfeld eine unterzeichnete Geheimhaltungserklärung des externen Partners einzuholen.
Das dauerhafte Öffnen von Verbindungen ist nicht erlaubt.

Fremde Geräte
Bitte beachten Sie, dass es nicht erlaubt ist:
unternehmensfremdes IT-Equipment (z. B. Grafik/TV-Karten, Festplatten, USB-Speichermedien) in firmeneigene Systeme einzubauen,
unternehmensfremdes IT-Equipment (z. B. private Rechner, Smartphones, USB-Speichermedien) in die IT-Infrastruktur (Datennetze, IT-Systeme etc.) des Unternehmens einzubinden oder datentechnisch direkt daran zu koppeln,
IT-Geräte von Kunden ohne Rücksprache mit der IT-Abteilung mit dem Unternehmensnetzwerk zu verbinden.

Das Gäste-WLAN ist von dieser Regelung ausgeschlossen.

Beim Kunden / Lieferanten
Nutzen Sie Kundennetzwerke (z.B. Verbindung in ein Produktionsnetzwerk) nur für den betrieblichen Zweck.

Remote Zugang / mobile Arbeit
Um Mitarbeitenden beim mobilen Arbeiten den Zugriff auf die Daten des Unternehmens zu ermöglichen, stellt das Unternehmen einen Remote Access-Zugang zur Verfügung. Mitarbeitende, die zur Nutzung dieses Zugangs berechtigt sind und auf deren Rechnern entsprechende Client-Software installiert wurde, können hierüber von jedem Ort, an dem sie über einen Internetzugang (z. B. DSL, WLAN usw.) verfügen, eine gesondert authentisierte und verschlüsselte Internet-Verbindung in die Datennetze des Unternehmens aufbauen.
Voraussetzung zur Einwahl ist ein Notebook das Ihnen durch die IT-Abteilung von unserem Unternehmen zur Verfügung gestellt wurde.

19. Vernichtung von Dokumenten

Vernichten Sie sensible Daten immer „sicher“ (z.B. Schredder oder Entsorgungsunternehmen).
Berücksichtigen Sie bei der Vernichtung von Dokumenten die Aufbewahrungsfristen.

20. Clean Desk Policy

Sperren Sie das Betriebssystem beim Verlassen des Arbeitsplatzes. Hilfreich ist hier die Tastenkombination „Windowstaste +L“.
Als Hilfestellung können Sie eine automatische Sperre des Rechners nach 10 oder 15 Minuten einstellen. Lassen Sie keine vertraulichen Informationen am Schreibtisch und

bei Auswärtstätigkeiten frei zugänglich liegen. Achten Sie beim Ausdruck sensibler Daten darauf, dass die Dokumente nicht für unberechtigte Dritte zugänglich sind.

21. Telefonie

Private Nutzung
Die private Nutzung der betrieblichen Mobiltelefone bzw. Festnetztelefone ist in Einzelfällen gestattet, wenn Sie sich damit einverstanden erklären, dass die Protokolle der Telefonie ausgewertet werden.
Nutzen Sie die Telefongeräte nicht privat, wenn Sie sich damit nicht einverstanden erklären. Beachten Sie die Verhältnismäßigkeit der Nutzung!

22. Kundeneigentum

Verwenden Sie Kundeneigentum nur zum vorgegebenen Zweck.
Führen Sie keine unautorisierten Änderungen an Kundeneigentum durch.

23. Austritt eines Mitarbeiters

Beim Ausscheiden aus dem Unternehmen sind alle Unternehmenswerte zurückzugeben.
Betriebliche E-Mails sind von allen privaten Geräten zu löschen.

24. Sicherheitsvorfälle

Sicherheitsvorfälle sind umgehend mitzuteilen, damit der größtmögliche Schaden vermieden werden kann. Wenden Sie sich dazu bitte an die IT-Verantwortlichen oder Ihre Führungskraft.
Beispiele:
Besteht die Vermutung, dass Accountdaten bekannt geworden sind, ist dieser Account sofort sperren zu lassen, bzw. das Passwort zu ändern.
Wurden interne oder vertrauliche Informationen unberechtigten Dritten zugänglich, ist sofort der zuständige Vorgesetzte zu informieren, um das weitere Vorgehen zu entscheiden.
Sind personenbezogene Daten unbefugt an Dritte geraten, ist auch die Datenschutzbeauftragte sofort zu informieren: datenschutz@mueller-hygiene.de

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Frau/Herr

wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlaubt oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen
auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden; für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“); sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden; in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungs - pflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.
Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

Ort, Datum	Unterschrift des Verpflichteten	Unterschrift des Verantwortlichen