Dienstanweisung IT-Sicherheit und Datenschutz

1. Geltungsbereich

Diese Dienstanweisung gilt für alle Beschäftigten. Dazu gehören alle Festangestellte, Teilzeitangestellte, Auszubildende, Werkstudenten, Aushilfskräfte, Praktikanten sowie Zeitarbeitnehmer etc. Auch externe Personen, die regelmäßig in unserem Betrieb tätig sind, sind verpflichtet, sich an diese Anweisungen zu halten.

2. Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme, Software und Applikationen in unserem Betrieb sind von den Beschäftigten die betrieblichen Regelungen und Dienstanweisungen sowie die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit einzuhalten. Gemäß Datenschutz Grundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG)

- ist es Ihnen gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.
- ist es Ihnen untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten, absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder unbefugtem Zugang führt.
- können Verstöße gegen die Datenschutzvorschriften gegebenenfalls mit Geld- oder Freiheitsstrafe geahndet werden.
- stellt ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.

Sollten Beschäftigte unsicher sein, ob und inwieweit Rechtsvorschriften oder betriebliche Regelungen einzuhalten sind, haben sie sich an die Geschäftsleitung bzw. an den Personalverantwortlichen zur Klärung zu wenden.

Die Verpflichtung auf Vertraulichkeit besteht auch nach der Beendigung des Beschäftigungsverhältnisses fort.

3. Ansprechpartner

Fallen IT-Systeme, Software oder Applikationen aus, sind defekt, zerstört, gehen verloren oder werden gestohlen, wird dies umgehend gemeldet. Das gilt auch für private Geräte, die dienstlich genutzt werden. Bei Fragen, Unsicherheiten, Verdacht auf Virenbefall oder Meldungen zu Vorfällen in der IT-Sicherheit und im Datenschutz, wenden sich die Beschäftigten an:

Administrator, intern	Constantin Held, Tel 02261-969317-14, constantin-held@skholzbau.de
Geschäftsführung	Martin Schwirten und Tobias Langusch, info@skholzbau.de
Datenschutzbeauftragter	KHBL Service- und Wirtschaftsgesellschaft mbH, Telefon: 02202 9359 – 620, E-Mail: datenschutz@service-handwerk.de

Die aktuellen Ansprechpartner können die Beschäftigten auch immer bei der Geschäftsleitung erfragen.

4. Schulung

Der Betrieb trägt Sorge dafür, dass die Beschäftigten die erforderlichen Schulungen, Instruktionen und Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen, Software und Applikationen erforderlich sind. Bei Bedarf ist eine Schulung/Fortbildung einzufordern.

5. Externe (Kunden, Besuchende)

Ein Zutritt externer Betriebsräume ist nur in Begleitung eines Beschäftigten gestattet. Telefonate und Akten sind vor Externen geheim zu halten. Externe dürfen sich ausschließlich über das Gäste-WLAN einwählen.

6. Allgemeine Regelungen

IT-Systeme, Telekommunikationseinrichtungen (insbesondere Internet, WLAN, Festnetz- und Mobiltelefone), Software, Applikationen und sonstige Anwendungen im Betrieb werden ausschließlich zu dienstlichen Zwecken und im jeweils erlaubten Umfang zur Aufgabenerledigung genutzt. Dies betrifft sowohl die Nutzung der Geräte an sich (PC, Laptop, Tablet, Smartphone, Kamera, etc.), Wechseldatenträger (externe Festplatte, USB-Stick, SD-Karte, CD/DVD, etc.) als auch den Internetanschluss. Alle Geräte müssen mit einem Passwortschutz gesichert werden. Die Geräte sollen sich – wenn dies technisch möglich ist – nach spätestens 10 Minuten zusätzlich selbst sperren.

Sollten Foto- und/oder Videoaufnahmen mit privaten Endgeräten für dienstliche Zwecke erstellt werden, sind diese umgehend nach Übermittlung an den Arbeitgeber zu löschen. Diese Aufnahmen dürfen nicht an Dritte verschickt werden.

Untersagt sind außerdem insbesondere

1. die Nutzung privater Hardware (PCs, Laptop, Tablets, Smartphones, Wechseldatenträger, etc.) zu dienstlichen Zwecken ohne Genehmigung des Arbeitgebers
2. die eigenmächtige Inbetriebnahme und/oder der Anschluss nicht zugelassener mobiler Wechseldatenträger (Externe Festplatte USB-Stick, SD-Karte, CD/DVD, etc.) an die IT-Systeme
3. die Nutzung privater und nicht für dienstliche Zwecke freigegebener Software
4. eigenmächtige Änderungen/Konfiguration an Hard- und/oder Software
5. Programme, Apps oder sonstige Software selbstständig zu installieren
6. Sicherheitseinrichtungen zu umgehen (z. B. Passwortschutz, Virenschutz, Firewall, Sicherheitssoftware)
7. Private Geräte zum Laden an die USB-Anschlüsse der betrieblichen IT und Hardware (PCs, Laptop, Tablets, Smartphones, etc.) anzuschließen
8. das Laden, Speichern und Bearbeiten privater Dokumente und Fotos
9. das Verarbeiten von betrieblichen Daten auf fremden IT-Systemen
10. die Verwendung der privaten Cloud-Speicher für Betriebsdaten
11. das Hinterlegen bzw. die Nutzung der dienstlichen E-Mail-Adresse (z.B. als Benutzername) in/für private Netzwerkdienste
12. Benutzerwechsel unter ein und derselben Benutzerkennung bei kurzen Unterbrechungen der Arbeit
13. Maßnahmen, die zur Verschlechterung des Datenschutzniveaus führen
14. nicht autorisierten Personen Zugang zu betrieblichen IT-Systemen zu verschaffen

Zudem gilt Folgendes:

15. Es werden keine kostenpflichtigen Informationen oder Leistungen für den Privatgebrauch zu Lasten des Betriebes abgerufen.
16. Es wird nicht gegen Rechte Dritter verstoßen, z.B. durch die unerlaubte Nutzung von Tauschbörsen.
17. Es wird kein eigener geschäftsmäßiger oder unternehmerischer Zweck verfolgt.
18. Spielen von Onlinespielen (da diese Schadcodes, Viren, Trojaner einbringen können) ist untersagt.
19. Es werden keine privaten Lieferungen an die Geschäftsadresse veranlasst.

7. Soziale Medien

Gehört zu den wahrzunehmenden dienstlichen Zwecken die Nutzung sozialer Netzwerke (z.B. Facebook, Instagram, etc.) oder anderer Online-Dienste, ist diese Nutzung gestattet. Hierfür ist der abgestimmte Benutzerzugang zu den sozialen Netzwerken oder Online-Diensten zu verwenden. Es ist untersagt, eine Firmen-Seite/Social-Media-Account ohne Absprache mit der Geschäftsführung zu erstellen/betreiben und/oder die zugehörigen Zugangsdaten zu ändern.

8. Private Nutzung

Sollte die private Nutzung notwendig sein, holen sich die Beschäftigten eine **schriftliche Ausnahmebestätigung** von der Geschäftsführung. Die Beschäftigten nutzen für den privaten Gebrauch (in Ihren Pausen) ausschließlich das vom Betrieb bereitgestellte Gäste-WLAN mit ihren privaten Geräten.

9. Mobile Endgeräte (Laptop, Tablet, Smartphone)

Mobile Endgeräte sind beliebte Ziele für Diebstähle. Die Beschäftigten achten darauf, dass diese sicher aufbewahrt werden. Insbesondere ist dabei zu beachten:

- Passwörter dürfen nicht schriftlich fixiert oder in der Nähe der Geräte oder damit zusammen aufbewahrt werden (siehe Punkt “Passwort”),
- nicht unbeaufsichtigt sein dürfen,
- nicht an Dritte weitergegeben werden dürfen,
- außerhalb der Nutzungszeiten weggeschlossen werden,
- bei Nichtnutzung wird immer der Zugriffsschutz („Windows- Taste + L“) aktiviert,
- die in einem Kraftfahrzeug aufbewahrt werden, von außen nicht sichtbar, abgedeckt oder in den Kofferraum eingeschlossen werden,
- keine extremen Temperaturen (z.B. in geparkten Kraftfahrzeugen) ausgesetzt werden. Insbesondere der Akku und das Display können dadurch beschädigt werden,
- vor schädlichen Umwelteinflüssen (Feuchtigkeit, Regen, Staub, etc.) geschützt werden,
- keinen starken mechanischen Beanspruchungen ausgesetzt werden,

- in Hotelräumen nicht unbeaufsichtigt herumliegen dürfen, sondern in einen Schrank oder Zimmersafe eingeschlossen werden,
- auch bei kürzeren Transportwegen möglichst stoßgeschützt (stabile Taschen/Koffer, Schutzhüllen) befördert und z.B. Laptops immer zusammengeklappt werden,

Außerdem

- sollten nicht benötigte Schnittstellen (z.B. Bluetooth, WLAN, etc.) bei Nichtnutzung deaktiviert werden.
- dürfen mobile Endgeräte nicht über den USB-Anschluss an unbekannten Quellen angeschlossen werden. Dies gilt insbesondere, um den Akku des Gerätes zu laden (z.B. öffentliche Ladestationen an Flughäfen).
- dürfen keine Wechseldatenträger und Geräte aus unbekannter Herkunft an die mobilen Endgeräte angeschlossen werden (z.B. Messegeschenke).
- sind Jailbreak (iOS) oder Rooting (Android) verboten.
- sind in der Regel ein Betriebssystem, eine Firewall und ein Antivirenprogramm installiert. Sofern die Aktualisierung dieser Systeme und Software nicht zentral durchgeführt wird, wird der Beschäftigte selbst für Aktualisierung sorgen.

10. Arbeitsplatz

Alle vertraulichen Dokumente, die sich auf einem Arbeitsplatz befinden, sind für unbefugte Personen (Reinigungspersonal, unbefugte Kolleginnen und Kollegen oder Besuchende) nicht zugänglich. Insbesondere gilt:

- auf dem Schreibtisch und dem virtuellen Desktop befinden sich grundsätzlich nur Akten und Dateien, die zur Bearbeitung des aktuellen Sachverhaltes dienen.
- In Bereichen mit Publikumsverkehr sind die IT-Systeme - insbesondere die Bildschirme - so auszurichten, dass das Risiko der Kenntnisnahme durch Besuchende oder Dritte nach Möglichkeit ausgeschlossen wird.
- Es werden keine ausgedruckten Daten mit vertraulichen Informationen in Drucker und Faxgeräte liegen gelassen.
- Papiermüll, der sensible oder vertrauliche Informationen enthält, wird in den dafür bereitgestellten Datenmüllbehältern bzw. Aktenvernichtern entsorgt. Diese Daten dürfen nicht in den üblichen Haus-/Papiermüll gelangen.
- Fenster und (Balkon-)Türen, werden, wenn der Arbeitsplatz nicht besetzt ist, verschlossen.
- Sobald ein Arbeitsplatz für längere Zeit nicht besetzt ist, werden alle sensiblen und vertraulichen Dokumente vom Schreibtisch entfernt und in einer Schublade oder einem Rollcontainer verstaut. Dies gilt auch für Speichermedien (wie USB-Sticks oder CDs) und mobile Endgeräte (Laptops, Tablets, Smartphones, etc.).
- In Bereichen mit Publikumsverkehr werden beim Verlassen der Büroräume die Türen abgeschlossen, insbesondere, wenn sich vertrauliche Informationen im Büroraum befinden.
- bei Nichtnutzung wird immer der Zugriffsschutz („Windows-Taste + L“) aktiviert.
- Bei Arbeitsende ist der PC herunterzufahren, Schreibtisch von offenliegenden Akten zu befreien, Fenster und Türen zu schließen, sämtliche mobilen Endgeräte und Wechseldatenspeichergeräte in Schubladen oder Rollcontainer zu verstauen. Die jeweiligen Schlüssel stecken nicht von außen an der Schublade oder dem Rollcontainer.

11. Home-Office

Arbeiten Beschäftigte im Home-Office ist das Schutzniveau der betrieblichen Anforderung (siehe insbesondere Punkte “Arbeitsplatz”) einzuhalten. Es erfolgt keine lokale Speicherung betrieblicher Daten auf privater IT.

- IT-Systeme (PCs, Laptops, Tablets, Smartphones) werden vor unbefugtem Zugang (einschließlich Familienangehöriger) geschützt.
- Vertrauliche Telefongespräche sind so zu führen, dass Familienangehörige oder sonstige im häuslichen Arbeitsbereich anwesende Personen sie nicht mithören können.
- Akten, Unterlagen und Datenträger müssen immer sicher transportiert und dürfen nicht unbeaufsichtigt gelassen werden.
- Nicht mehr benötigte Unterlagen werden (über einen Aktenvernichter) vernichtet und dürfen nicht über den Haus-/Papiermüll entsorgt werden. Alternativ werden die Unterlagen im Betrieb entsorgt.
- bei Nichtnutzung wird immer der Zugriffsschutz („Windows- Taste + L“) aktiviert.
- Bei längerem Verlassen des Home-Office bzw. der Wohnung
  - > werden die IT-Systeme heruntergefahren.
  - > werden Türen und Fenster sicher verschlossen.
- Bei Gewitter, Stromausfall oder längerer Abwesenheit (Urlaub usw.) werden Netz- und Datenleitungen von den Anschlussdosen getrennt.

- Das Betriebssystem sowie installierte Programme (insbesondere Firewall, Virenschutz-Programme) und Apps werden regelmäßig aktualisiert.
- Der WLAN-Router im Home-Office wird durch ein (neues) mindestens 16 Zeichen langes Passwort (gem. Punkt "Passwort") vor unerlaubtem Zugriff gesichert.
- Bei technischen Störungen (Hard- oder Software) wird sofort der entsprechende Ansprechpartner für die IT-Sicherheit in Kenntnis gesetzt.
- Den Beschäftigten ist bewusst, dass die IT-Abteilung die Möglichkeit zur Fernwartung für Support und Administrationszwecke erhält. Der Zugriff erfolgt immer in Absprache.

12. E-Mail-Nutzung

Der bereitgestellte E-Mail-Account darf nur für betriebliche Zwecke genutzt werden. Beschäftigte beachten bei der E-Mail-Kommunikation folgende Punkte:

- Berufliche E-Mails oder elektronische Besprechungseinladungen dürfen nicht auf private E-Mail-Postfächer weitergeleitet werden.
- Der Empfänger einer E-Mail ist vor dem Versand nochmals als Berechtigter zum Erhalt der enthaltenen Information zu prüfen.
- Die Felder „CC:" und „BCC:" werden korrekt verwendet.
- Keine Öffnung von E-Mails, wenn Absender oder Betreffzeile verdächtig erscheinen.
- Unbekannte oder unerwünschte E-Mails mit Anhängen sind in keinem Fall zu öffnen und umgehend ungelesen zu löschen. Die entsprechenden Anhänge werden nicht geöffnet.
- Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern wird hinterfragt:
  - > Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)?
  - > Erwartet man die beigefügten Dateien und passen sie zum Absender, oder kommen sie völlig unerwartet?
- Phishing-Mails, die z.B. zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (PIN, TAN, etc.) auffordern, werden gelöscht. Die angeforderten, vertraulichen Informationen dürfen auf keinen Fall weitergegeben werden.
- E-Mail-Links sollten nicht angeklickt werden, um eine Webseite aufzurufen. In betrügerischen E-Mails wird hinter diesem Link eine völlig andere Internet-Adresse hinterlegt, als in der Mail zu sehen ist. Beim Anklicken wird eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert.
- Spam-Mails dürfen nicht beantwortet werden. Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit der Mail-Adresse und erhöht das Risiko weiterer Zusendungen.
- **Bei Fragen und Unsicherheiten sollte immer der Ansprechpartner für die IT-Sicherheit kontaktiert werden.**

13. Social Engineering

Unter Social Engineering versteht man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Vorwiegend wird dieser Angriff per Telefon oder E-Mail durchgeführt.

- Es werden keine vertraulichen Informationen per Telefon oder E-Mail weitergegeben.
- Die Kommunikation personenbezogener Daten erfolgt ausschließlich an eindeutig authentifizierte Personen.
- Behörden werden in keinem Fall die mündliche Herausgabe von Daten verlangen („falsche Polizeianrufe …").
- Bei ungewöhnlichen Anweisungen durch Vorgesetzte werden diese auf einem zweiten Kommunikationsweg um Bestätigung gebeten.
- Vorsicht bei Telefonanrufen oder E-Mails von vermeintlichen „Kollegen", speziell wenn der Wunsch oder der Auftrag außergewöhnlich ist. Mit dem entsprechenden Kollegen sollte auf einem anderen Kommunikationsweg persönlich Kontakt aufgenommen werden.
- Bei nicht eindeutig identifizierten Kommunikationspartnern erfolgt nur schriftliche Auskunft an die im Verwaltungsprogramm hinterlegte Adresse.
- Übt die betroffene Person Druck zur Herausgabe von Daten aus, ist der Vorgesetzte zu informieren.

14. Entsorgung und Reparatur

Dokumente, mobile Wechseldatenträger (externe Festplatte, USB-Stick, SD-Karte, CD/DVD, etc.) und IT-Systeme (PC, Laptop, Tablet, Smartphone aber auch Drucker, Faxgeräte) werden sicher entsorgt. Es sind keine Rückschlüsse mehr auf vorher gespeicherte Daten möglich.

- Außer Sichtprüfungen (z.B. Kabel entfernt) sind keine eigenständigen Reparaturversuche zu unternehmen.
- Nicht mehr benötigte Datenträger und IT-System müssen zurückgegeben werden.
- Datenträger, wichtige Dokumente oder IT-Systeme werden nicht im Haus-/Papiermüll entsorgt.

15. Diebstahl und Verhalten bei Sicherheitsvorfällen

Das Auftreten von sicherheitsrelevanten Ereignissen ist unverzüglich mitzuteilen. Dazu zählen unter anderem:

- Diebstahl, Verlust, Abhandenkommen und Missbrauch von IT-Systeme (Laptop, Tablet, Smartphone, Kamera, Drohnen, etc.) und Wechseldatenträger (externe Festplatten, USB-Stick, SD-Karte, CD/DVD etc.),
- Verlust oder Veränderung von Dateien,
- Verdacht auf Missbrauch von Benutzername und Passwort,
- unerklärliches Systemverhalten und
- Infizierung mit einem Computervirus.

16. Meldung von möglichen Datenschutzvorfällen

Mögliche Datenschutzvorfälle werden unverzüglich der Geschäftsführung gemeldet. Ein Datenschutzvorfall liegt insbesondere vor, wenn

- die Annahme besteht, dass die Datensicherheit, insbesondere die Vertraulichkeit von Daten, gefährdet ist.
- die Möglichkeit nicht auszuschließen ist, dass Daten abhanden gekommen sind, oder Dritte unbefugt Zugriff oder Zugang zu personenbezogenen Daten haben oder hatten.

17. Passwort

Dienstliche Endgeräte (Computer, Mobiltelefone, iPads, etc.) müssen durch ein Passwort oder einen anderen Schutzmechanismus vor unbefugtem Zugriff geschützt werden.

1. Für unterschiedliche Zugänge werden unterschiedliche Passwörter verwendet.
2. Es werden keine Passwortnotizen am Arbeitsplatz aufbewahrt.
3. Passwörter sind geheim zu halten. Sie sind verdeckt einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt oder unverschlüsselt auf Rechnern gespeichert werden.
4. Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Zu vermeiden sind insbesondere:
    - Vor- und Familiennamen, Telefonnummern, Geburtstage sowie Namen von Angehörigen
    - Trivial angeordnete Zahlenkombinationen (z.B. 12345)
    - Zeichenwiederholungen (z.B. 1111111)
    - Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen
    - Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden (z.B. QWERTZ)
    - Zeichenkombinationen, die Suchbegriffe in Wörterbüchern und Lexika entsprechen, Eigennamen und geografische Begriffe (Trivialpasswörter)
5. Passwörter werden unverzüglich gewechselt, wenn der Verdacht besteht, dass diese bekannt geworden sind.

Name in Druckbuchstaben

Datum, Unterschrift