Template A0
IT Sicherheitsleitlinie
- Handwerk

Herausgeber:

Handwerkskammer Rheinhessen

Dagobertstraße 2
55116 Mainz

Telefon: (06131) 9992 – 61
Telefax: (06131) 9992 – 861
E-Mail: j.schueler@hwk.de
Webseite: www.it-sicherheitsbotschafter.de

Stand: Juni. 2020

Inhalt

1 Einleitung

Unser Unternehmen ist ein innovativer Dienstleister im Handwerk [*Geschäftszweck*]. Wir beschäftigen [*Mitarbeiter*]. [*Ort*] ist unser einziger Standort. *[Ergänzen könnte man noch Informationen über die Art der Kunden und die Bedeutung der Sicherheit für einzelne Kunden und Aufträge.]*

1.1 Die IT-Sicherheitsleitlinie

Die Leitlinie zur Informationssicherheit beschreibt allgemeinverständlich, was Informationssicherheit ist und welche Bedeutung sie für unser Unternehmen hat. Das Dokument zeigt auf, wie Informationssicherheit im Unternehmen gelebt wird, indem das zu erreichende Mindest-Sicherheitsniveau beschrieben wird sowie die angestrebten Informationssicherheitsziele und die verfolgte Informationssicherheitsstrategie dargestellt werden.

1.2 Geltungs-/Anwendungsbereich

Der Wettbewerb und Kunden verlangt neben der Produktion und Lieferung qualitativer Produkte auch den Nachweis der Qualität und Sicherheit interner Prozesse. Die vorliegende Informationssicherheitsleitlinie adressiert dieses Erfordernis im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb unseres Unternehmens. Sie gilt somit für das gesamte Unternehmen.

- Diese Leitlinie richtet sich an alle Mitglieder und Angehörige des Unternehmens. Hierzu zählen auch die Beschäftigten von beauftragten Dienstleistungsunternehmen und Geschäftspartnern.
- Jeder Beschäftigte ist verpflichtet, die IT-Sicherheitsleitlinie im Rahmen seiner Zuständigkeiten und Arbeiten einzuhalten und die Informationen und die Technik angemessen zu schützen.
- Unter den Vorgaben dieser IT-Sicherheitsleitlinie und dem IT-Grundschutzprofil für Handwerksbetriebe werden Ziele, Anforderungen, organisatorische und technische Sicherheitsmaßnahmen in dem IT-Sicherheitskonzept detailliert geplant, dokumentiert und dann umgesetzt.

2 Definitionen und Erläuterungen

Bei der Gestaltung von Informationssicherheit orientiert sich unser Unternehmen an dem IT-Grundschutzprofil für Handwerksbetriebe und den Empfehlungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

2.1 Grundwerte der Informationssicherheit

Aufgabe der Informationssicherheit ist der angemessene Schutz der drei Grundwerte.

- ***Integrität***
  Mit diesem Begriff wird die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen bezeichnet. Bei intakter Integrität sind

Daten vollständig und unverändert. Eventuell zugehörige Attribute wurden nicht unerlaubt manipuliert.

- ***Verfügbarkeit***
  Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
- ***Vertraulichkeit***
  Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen, aber auch der Zutritt zu Räumlichkeiten dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Die Einhaltung weiterer Grundwerte wird für personenbezogene Daten durch den Datenschutz geprüft

2.2 Anforderungen, Risiken und Ziele

Das Vertrauen unserer Kunden und letztlich unser Geschäftserfolg beruhen darauf, dass wir insbesondere

- die gesetzlichen Vorgaben und hier nicht zuletzt die Datenschutzgesetze einhalten (Compliance),
- unsere Betriebsgeheimnisse schützen,
- die Vertraulichkeit der Daten unserer Kunden wahren,
- unsere Projekte und Dienstleistungen in der geplanten bzw. zugesicherten Zeit abwickeln,

Vor diesem Hintergrund ist der Geschäftserfolg unseres Unternehmens davon abhängig, dass wir bestehende Risiken für die genannten Ziele erkennen, durch geeignete Maßnahmen vermeiden bzw. mindern und verbleibende Risiken geeignet behandeln.

Zu den Risiken zählen die unvollständige bzw. nicht korrekte Einhaltung von gesetzlichen Vorgaben, die unbefugte und ggf. unbemerkte Weitergabe von Betriebsgeheimnissen, die Verletzung von Vorgaben unserer Kunden aufgrund von Systemausfall, Datenverlust sowie unbefugter Preisgabe von Informationen.

3 Bedeutung der Informationssicherheit für das Unternehmen

3.1 Stellenwert der Informationssicherheit

Die Unternehmensleitung schätzt die strategische und operative Bedeutung der Informationstechnik folgendermaßen ein:

> Die Informationstechnik dient unserem Unternehmen wesentlich zur Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung und Abrechnung sowie für die Aufgaben der Finanz- und Lohnbuchhaltung. Insbesondere für auftragsbezogene Entscheidungen und Investitionen sind aktuelle und korrekte Unternehmensdaten erforderlich. Ein Ausfall von IT-Systemen ist bis zu einem Tag überbrückbar, darüber hinaus wären Beeinträchtigungen der Auftragsabwicklung und der Unternehmenskommunikation zwischen Verwaltung, Großhändler und Kunden riskant.

Vor dem Hintergrund der externen und internen Anforderungen, vor allem aber den Sicherheitsanforderungen unserer Kunden muss Informationssicherheit ein integraler Bestandteil unserer Unternehmenskultur sein.

Jeder Mitarbeiter / jede Mitarbeiterin muss sich der Notwendigkeit der Informationssicherheit bewusst sein und die grundsätzlichen Auswirkungen von Risiken auf den Geschäftserfolg kennen.

Neben der Abwehr dieser Angriffe auf Daten und Systeme ist die Aufrechterhaltung des Geschäftsbetriebs ein wesentliches Ziel der Informationssicherheit. Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit ihr sind wesentliche Voraussetzungen für die Einhaltung der IT-Sicherheitsziele Verfügbarkeit, Integrität und Vertraulichkeit von Informationen.

Durch die Umsetzung von Sicherheitsmaßnahmen soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheit geboten wird, um Informationswerte und personenbezogene Daten zu schützen und die Verfügbarkeit zu gewährleisten.

Die Unternehmensleitung hat aufgrund ihrer Verantwortung für die Informationssicherheit einen IT-Sicherheitsprozess in Gang gesetzt. Dazu gehören die Entwicklung und Umsetzung dieser Leitlinie und eines IT-Sicherheitskonzepts. Die Einhaltung der Leitlinie sowie Aktualität und Angemessenheit des Sicherheitskonzepts werden regelmäßig überprüft.

3.2 Leitsätze der Informationssicherheit (Mindestsicherheitsniveau)

In Abwägung der Gefährdungen, der Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für IT-Sicherheit, hat die Unternehmensleitung bestimmt, dass ein **grundlegendes IT-Sicherheitsniveau** angestrebt werden soll. Das Unternehmen orientiert sich an den folgenden Leitsätzen:

1. Das Unternehmen orientiert sich bei der Ausgestaltung ihres Informationssicherheits-prozesses am IT-Grundschutzprofil für Handwerksbetriebe.
2. Der Erfolg von Informationssicherheit kann nur gewährleistet werden, wenn im ganzen Unternehmen einheitliche und angemessene Sicherheitsstandards im Sinne eines Mindeststandards definiert und etabliert werden:
3. Die Etablierung eines umfassenden Informationssicherheitsprozesses wird durch die Unternehmensleitung initiiert und aktiv unterstützt.
4. Aufwand (finanziell wie personell) und Ziele von Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinander stehen.
5. Ziel von Informationssicherheit im Unternehmen ist es, einen Zustand zu erreichen bzw. zu erhalten, in dem die Grundwerte der Informationssicherheit entsprechend der Vorgaben der Unternehmensleitung und bestehender rechtlicher Auflagen gewahrt werden und die potentiellen Bedrohungen nur so wirksam werden können, dass die verbleibenden Risiken tragbar sind. Der Fokus liegt dabei auf Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit des jeweiligen Zielobjekts. Das bedeutet, dass auch im Umgang mit elektronischen Dokumenten und Daten Geheimhaltungsanweisungen strikt Folge zu leisten ist.
6. Die für das Unternehmen relevanten Gesetze und Vorschriften sowie vertragliche und aufsichtsrechtliche Verpflichtungen müssen eingehalten werden.

7. Ziel ist, die Sicherheit der IT (gleichwertig neben Leistungsfähigkeit und Funktionalität) im Unternehmen aufrechtzuerhalten, so dass die Geschäftsinformationen bei Bedarf verfügbar sind. Ausfälle der IT haben Beeinträchtigungen des Unternehmens zur Folge. Lang andauernde Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag führen, sind nicht tolerierbar.
8. Durch Sicherheitsmängel im Umgang mit IT verursachte Ersatzansprüche, Schadensregulierungen und Image-Schäden müssen verhindert werden. [Kleinere Fehler können toleriert werden.]
9. Im Unternehmen sollen für die Zugangskontrolle sowohl physikalische als auch logische Sicherheitsmaßnahmen angewandt werden.
10. Bereits betriebene und geplante Informationstechnik soll nach der Vorgehensweise des IT-Grundschutzprofils für Handwerksbetriebe in einem IT-Sicherheitskonzept erfasst, im Schutzbedarf eingeschätzt, modelliert und auf Sicherheitsmaßnahmen überprüft werden. Sicherheit der IT soll u. a. auch durch Anwenden von Normen und Standards und durch den Einsatz zertifizierter Systeme erreicht werden.
11. Informationssicherheit ist eine Gemeinschaftsaufgabe, die von allen Nutzerinnen/Nutzern der IT-Infrastruktur wahrgenommen werden muss. Eine erfolgreiche Umsetzung ist nur durch eine offene Kommunikation und Sensibilisierung der Nutzerinnen/Nutzer sowie durch Einhaltung der Sicherheitsrichtlinien möglich
12. Informationssicherheit soll mit Sicherheitsbewusstsein der Beschäftigten bezüglich möglicher Gefährdungen und mit ihrem persönlich-verantwortlichen Verhalten praktiziert und mit organisatorischen und technischen Maßnahmen unterstützt werden. Dafür sollen regelmäßige Fortbildungsmaßnahmen zur IT-Sicherheit durchgeführt werden.
13. Die Mitarbeiter/innen unseres Unternehmens erhalten bei Bedarf für den jeweiligen Arbeitsplatz spezielle Sicherheitsregeln, die insbesondere eine Meldepflicht bei Sicherheitsvorkommnissen beinhalten.
14. Alle Mitarbeiter/innen haben regelmäßig an den angebotenen Sicherheitsschulungen teilzunehmen
15. Jeder Mitarbeiter / jede Mitarbeiterin ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu beachten und einzuhalten.
16. Die vorliegende Sicherheitsleitlinie ist grundsätzlich nur unternehmensintern zu halten. Bei Bedarf wird die Leitung darüber befinden, ob sie an Dritte (z. B. Kunden, Vertragspartner, Lieferanten) weitergegeben werden kann.

Informationssicherheit ist kein einmaliges Projekt. Informationssicherheit ist ein Prozess, der die Überwachung und Weiterentwicklung der Sicherheitsstandards erfordert. Zur Erfüllung ist die Einführung von Qualitätssicherungsmaßnahmen notwendig. Hierzu werden seitens der Unternehmensleitung alle erforderlichen Maßnahmen getroffen.

4 Informationssicherheitsleitlinie

4.1 Angestrebte Informationssicherheitsziele

Daher verfolgt das Unternehmen mit Fokus auf Bewahrung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität die folgenden allgemeingültigen Informationssicherheitsziele:

- Zuverlässige Unterstützung des Geschäftsbetriebs und der Geschäftsprozesse durch den IT-Beauftragten/-Dienstleister
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb des Unternehmens

- Schutz von Daten und Informationen unter Berücksichtigung ihrer spezifischen Anforderungen (personenbezogene Daten, Angebots-, Abrechnungsdaten usw.)
- Schutz der Infrastruktur gegen Missbrauch von innen und außen
- Einhaltung gesetzlicher Vorgaben zum Umgang mit Informationen und Systemen
- Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der IT-gestützten Verarbeitung personenbezogener Daten
- Aufrechterhaltung der positiven Außendarstellung.

4.2 Sicherheitsniveau

Ziel von Informationssicherheit des Unternehmens ist es, mindestens ein Sicherheitsniveau zu erreichen, das für den grundlegenden Schutzbedarf der Informationen angemessen und ausreichend ist. Die hierzu umzusetzenden Maßnahmen liefern einen soliden grundlegenden Schutz für alle Daten und die verbundenen Komponenten.

4.3 Verfolgte Informationssicherheitsstrategie

Die Informationssicherheitsstrategie wird durch die Geschäftsleitung festgelegt. Das Unternehmen orientiert sich bei der Gestaltung von Informationssicherheit am IT-Grundschutzprofil für Handwerksbetriebe. Eine Zertifizierung wird zurzeit nicht angestrebt.

Um das definierte Sicherheitsniveau des Unternehmens aufrecht zu erhalten, ist eine fortlaufende Kontrolle und Verbesserung der implementierten Sicherheitsmaßnahmen, Dokumente und des festgelegten Informationssicherheitsprozesses zwingend erforderlich. Dazu wird die Leitlinie zur Informationssicherheit mindestens alle zwei Jahre überprüft und aktualisiert.

4.4 Informationssicherheitsorganisation

4.4.1 Verantwortung

- Der Inhaber ist für die Einschätzung der geschäftlichen Bedeutung (der Information, Technik), für die sichere Nutzung und Kontrolle, inklusive der Einhaltung von Sicherheitsgrundsätzen, Standards und Richtlinien verantwortlich. Die „Inhaber", auch als Informationseigentümer bezeichnet definieren die erforderliche Zugänglichkeit (der Information, Technik) sowie Art und Umfang der Autorisierung. Er ist für die Verwaltung der zustehenden Zugriffsrechte der Benutzer verantwortlich und rechenschaftspflichtig.
- Ein IT-Dienstleister, der z. B. aufgrund eines Serviceauftrags für das Unternehmen Leistungen erbringt, hat Vorgaben des „Informationseigentümers" und diese IT Sicherheitsleitlinie einzuhalten. Damit ist er verantwortlich für die Einhaltung der IT Sicherheitsziele (Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Rechenschaftspflicht und Verbindlichkeit der Informationen). Bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen hat er den „Informationseigentümer" zu informieren.
- Jeder Mitarbeiter soll im Rahmen seines Umgangs mit IT (als Benutzer, Berater, Geschäftspartner) die erforderliche Integrität und Vertraulichkeit von Informationen sowie Verbindlichkeit und Beweisbarkeit von Geschäftskommunikation gewährleisten und die Richtlinien des Unternehmens einhalten. Unterstützt durch sensibilisierende Schulung und Benutzerbetreuung am Arbeitsplatz soll jeder im Rahmen seiner Möglichkeiten,

Sicherheitsvorfälle von innen und außen vermeiden. Erkannte Fehler sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

- Das Sicherheitsmanagement, bestehend aus Inhaber, IT-Beauftragtem und IT-Dienstleister, ist gemäß den Sicherheitsvorgaben verantwortlich für die Sicherheit im Umgang mit der IT und den Schutz der Geschäftsinformationen, einschließlich der Kunden- und Managementdaten. Ebenso ist es zuständig für die Weiterentwicklung des IT-Sicherheitsniveaus, des IT-Sicherheitskonzepts und für seine Umsetzung und Aufrechterhaltung von Sicherheit im Betrieb.
- Für die Überprüfung der IT-Sicherheit bei der Bearbeitung, Nutzung und Kontrolle von Informationen werden jeweils unabhängige Verantwortliche eingesetzt, die z. B. Zugriffsmöglichkeiten und zugehörige Sicherheitsmaßnahmen kontrollieren.

4.4.2 Verstöße und Folgen

- Beabsichtigte oder grob fahrlässige Handlungen, die die Sicherheit von Daten, Informationen, Anwendungen, IT-Systemen oder des Netzes gefährden, werden als Verstöße verfolgt. Dazu gehören beispielsweise:
  - der Missbrauch von Daten, der finanziellen Verlust verursachen kann, unberechtigte Zugriff auf Informationen bzw. ihre Änderung und unbefugte Übermittlung,
  - die illegale Nutzung von Informationen aus dem Unternehmen,
  - die Gefährdung der IT-Sicherheit der Mitarbeiter, Geschäftspartner und des Unternehmens und
  - die Schädigung des Rufes des Unternehmens.
- Bewusste Zuwiderhandlungen gegen die IT-Sicherheitsleitlinie werden bestraft – gegebenenfalls disziplinarisch, arbeitsrechtlich oder mit zivil- und strafrechtlichen Verfahren, in denen auch Haftungsansprüche und Regressforderungen erhoben werden können.

5 Schlusswort

Funktionierende und sichere Geschäftsprozesse sind eine maßgebliche Voraussetzung für die Leistungsfähigkeit des Unternehmens. Wenn die Grundregeln im Umgang mit Informationen und der IT als Werkzeug zu deren Verarbeitung eingehalten werden, werden damit der Bestand des Unternehmens, aber auch die Arbeitsplätze Mitarbeiter gesichert. Die Unternehmensleitung ist sich ihrer Verantwortung für die Informationssicherheit bewusst und unterstützt daher nachdrücklich jegliche Bemühungen. Das wertvollste Glied in dieser Kette ist jedoch der gesunde Menschenverstand jeder einzelnen Nutzerin, jedes einzelnen Nutzers und Ihre persönliche Bereitschaft, einen Beitrag zur Informationssicherheit leisten.

6 In-Kraft-Treten

Diese Leitlinie tritt mit sofortiger Wirkung in Kraft.