meteoviva

Leitlinie zur Informationssicherheit

Inhalt

1 Einleitung

Als SaaS (Software as a Service) Anbieter spielt die automatisierte Informationsverarbeitung eine Schlüsselrolle in der Leistungserbringung der meteoviva GmbH. Daher sind Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten von existentieller Bedeutung für Erfolg, Ansehen und Fortbestand des Unternehmens. Vor diesem Hintergrund ist ein angemessenes Niveau der Informationssicherheit in den Geschäftsprozessen der meteoviva GmbH zu organisieren.

Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit trägt die Geschäftsführung der meteoviva GmbH. Sie ist insbesondere verantwortlich für

- die Schaffung organisatorischer Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit,
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse,
- die Einrichtung eines Informationssicherheits-Managements,
- die Umsetzung der vereinbarten Sicherheitsmaßnahmen einschließlich der Bereitstellung der erforderlichen Haushaltsmittel,
- eine hinreichende und geeignete Dokumentation der IT-Infrastruktur sowie aller Sicherheitsvorkehrungen und Sicherheitsmaßnahmen,

Die meteoviva GmbH hat entsprechend den Anforderungen der internationalen Norm DIN ISO/IEC27001:2013 ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut, verwirklicht, erhält es aufrecht und verbessert es kontinuierlich.

Die vorliegende Leitlinie beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, welche für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind.

Die Begriffe „Daten“ und „Informationen“ werden in dieser Leitlinie synonym benutzt. Während mit Daten oftmals „Rohdaten/unverarbeitete Daten“ und mit Informationen „verarbeitete/aggregierte

Daten“ gemeint sind, so wird bezüglich der Informationssicherheit kein Unterschied zwischen Daten und Informationen gemacht.

2 Geltungsbereich

Diese Leitlinie gilt für alle Mitarbeiter und deutschen Standorte der meteoviva GmbH. Die Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen sind von allen Mitarbeitern der meteoviva GmbH zu beachten und einzuhalten. Bei Nichtbeachtung behält sich die meteoviva GmbH arbeitsrechtliche Schritte vor.

3 Grundsätze und Ziele der Informationssicherheit

3.1 Grundsätze

Informationssicherheit bezeichnet die angemessene Aufrechterhaltung der Sicherheitsziele Vertraulichkeit, Authentizität und Verfügbarkeit für Informationen und zugeordnete physische, technische und personelle Werte entsprechend den geschäftlichen, gesetzlichen und regulatorischen Anforderungen der meteoviva GmbH. Dabei ist es unerheblich, in welcher Darstellungsform die Informationen vorliegen.

Dies beinhaltet insbesondere die Analyse und Behandlung von Risiken, welche die o.g. Sicherheitsziele gefährden und durch die Umsetzung angemessener Maßnahmen auf ein akzeptierbares Maß reduziert werden. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen. Dabei bedeuten:

- **Vertraulichkeit**: Vertrauliche Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Nachrichteninhalte, die näheren Informationen über den Kommunikationsvorgang (wer, wann, wie lange, mit wem etc.) sowie die Daten über den Sende- und Empfangsvorgang.
- **Integrität**: Der Begriff der Integrität bezieht sich sowohl auf Informationen als auch das gesamte IT-System. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. Zum anderen bezieht sich der Begriff Integrität auch auf IT-Systeme, da die Integrität der Informationen und Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung sichergestellt werden kann.
- **Verfügbarkeit**: Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen stehen dem Anwender zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

Es ist das erklärte Ziel der meteoviva GmbH, dass alle Einrichtungen, die der Erstellung, Speicherung, Sicherung, Verarbeitung und Übertragung von Daten dienen, so ausgewählt, integriert und konfiguriert sind, dass für die auf ihnen verarbeiteten Daten zu jeder Zeit und unter allen Umständen das angemessene Maß an Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt ist. Dies schließt ausdrücklich alle beteiligten Mitarbeiter sowie deutschen Standorte mit ein. Belange der Informationssicherheit sind zu berücksichtigen bei

- der Klassifizierung, Kennzeichnung, Handhabung, Übertragung und dem Schutz von Informationen,
- der Steuerung des Zugangs zu Informationen,

- der Entwicklung, Einführung, Betrieb und Pflege von Produkten,
- der Personalsicherheit,
- der Beschaffung und Beseitigung / Entsorgung von IT-Produkten,
- der Nutzung von Diensten Dritter,
- der Handhabung von Informationssicherheitsvorfällen und Notfällen
- Change-Management Prozessen

Technische und organisatorische Sicherheitsmaßnahmen sind so zu gestalten, dass diese stets integraler Bestandteil aller Geschäftsprozesse sind. Belange der Informationssicherheit sind zu berücksichtigen

- in der Gestaltung der Organisation,
- bei der Schaffung und Besetzung von Funktionen und Rollen,
- in der Führung, Aus- und Weiterbildung von Mitarbeitern,
- der Gestaltung von Management,- Kern- und Unterstützungsprozessen,
- der Zusammenarbeit mit anderen Behörden und Externen,
- der Auswahl und dem Einsatz von Hilfsmitteln,
- der Entwicklung und Bereitstellung von Produkten und Dienstleistungen.

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser wird durch den Wert der zu schützenden Informationen und der IT-Systeme definiert. Zu bewerten sind dabei in der Regel die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigungen des Ansehens und die Folgen von Gesetzesverstößen. Für die Umsetzung der erforderlichen und angemessenen Sicherheitsmaßnahmen sind die notwendigen Ressourcen (Personal, Sach- und Investitionsmittel) bereit zu stellen.

- Wenn Angriffe auf die Sicherheit der IT-Infrastruktur der meteoviva GmbH drohen oder bekannt werden oder sonstige Sicherheitsrisiken auftreten, kann die Verfügbarkeit von IT-Anwendungen, Daten und Netzwerken entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der gesamten Unternehmung ist der Schutz vor Schäden vorrangig. Vertretbare Einschränkungen in Bedienung und Komfort sind hinzunehmen. Dies gilt in besonderem Maße für die Übergänge zu anderen Netzwerken, insbesondere zum Internet.
- Die Mitarbeiter sind im erforderlichen Umfang bezüglich der Informationssicherheit zu sensibilisieren und zu qualifizieren.

3.2 Ziele

Die in den nachfolgenden Abschnitten genannten Ziele dienen dazu, die an meteoviva gestellten gesetzlichen, regulatorischen und vertraglichen Anforderungen zu erfüllen. Sie werden mindestens jährlich überprüft und bei Bedarf aktualisiert.

3.2.1 Vertraulichkeit

Die in IT-Systemen erhobenen, gespeicherten, verarbeiteten und weiter gegebenen Daten sind entsprechend ihrer Klassifizierung vertraulich zu behandeln und jederzeit vor unbefugtem Zugriff zu

schützen. Zu diesem Zweck ist für alle Daten der Personenkreis, dem der Zugriff gestattet werden soll, zu bestimmen. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. Jeder Mitarbeiter erhält eine Zugriffsberechtigung nur auf die Daten, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt.

3.2.2 Authentizität

Die in IT-Systemen erhobenen, gespeicherten, verarbeiteten und weiter gegebenen Daten sollen jederzeit ihrem Ursprung zugeordnet werden können, damit die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit sichergestellt werden können.

3.2.3 Integrität

Informationen und Software-Produkte sind gegen unbeabsichtigte Veränderung und vorsätzliche Verfälschung zu schützen. Alle Software-Produkte sollen stets aktuelle und vollständige Informationen liefern. Eventuelle verfahrens- oder informationsverarbeitungsbedingte Einschränkungen sind zu dokumentieren.

3.2.4 Verfügbarkeit

Für alle in der Produktion eingesetzten IT-Systeme sind die Zeiten, in denen sie verfügbar sein sollen, festzulegen. Betriebsunterbrechungen sind in diesen Zeiten weitgehend zu vermeiden, d. h. nach Zahl und Dauer zu begrenzen. Die Beschreibung der notwendigen Verfügbarkeit umfasst

- die regelmäßigen Betriebszeiten,
- die maximal tolerierbare Dauer einzelner Ausfälle.

Ebenfalls festzulegen sind regelmäßig geplante Auszeiten, insbesondere zu Wartungszwecken.

4 Verantwortlichkeiten

4.1 Geschäftsführung

Die Geschäftsführung der meteoviva GmbH übernimmt die Gesamtverantwortung für das ISMS. Sie erlässt verbindliche Regeln zur Informationssicherheit und gibt sie den Mitarbeitern bekannt. Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher.

4.2 Mitarbeiter

Alle Mitarbeiter gewährleisten die Informationssicherheit durch verantwortungsbewusstes Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsvoll mit den von ihnen genutzten IT-Systemen, Daten und Informationen um.

4.3 Externe Leistungserbringer

Personen und Unternehmen, die nicht zur meteoviva GmbH gehören, für diese aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie einzuhalten. Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung. Dazu gehört auch, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren hat.

5 Informationssicherheitsorganisation

5.1 Beauftragter für Informationssicherheit

Die meteoviva GmbH ernennt einen Informationssicherheitsbeauftragten (ISB), der für alle Belange und Fragen der Informationssicherheit zuständig ist. Es ist sicher zu stellen, dass diesem Beschäftigten ein angemessener Teil seiner Arbeitszeit für die Erledigung seiner Aufgaben als ISB zur Verfügung steht.

Neben dem ISB wird ein Sicherheitsmanagement-Team mit je einem Mitarbeiter aus jeder Abteilung benannt, die bei der Umsetzung und Einhaltung der Informationssicherheit in ihrem jeweiligen Bereich eine Führungsrolle einnehmen.

6 Umsetzung

Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte und detaillierter Regelungen und Dienstanweisungen zur Informationssicherheit. Ihre Umsetzung erfolgt im Rahmen eines IS-Prozesses und einer Zertifizierung nach ISO 27001.

7 Kontinuierliche Verbesserung

Der Informationssicherheitsprozess ist regelmäßig auf seine Aktualität und Wirksamkeit zu überprüfen. Dies schließt u.a. eine regelmäßige Revision der aktuellen Risikobewertung- und -behandlung ein. Insbesondere sind die umgesetzten Maßnahmen regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Mitarbeitern bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

Die Leitungsebene verpflichtet sich zur ständigen Verbesserung des Sicherheitsniveaus.

Die Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit zu verbessern und ständig auf dem aktuellen Stand zu halten.

8 Unterschriften der Geschäftsführung

Jülich, 05.04.2024

Digital unterschrieben von Stefan Hardt
Ort: Jülich

Dr. Stefan Hardt

Digital unterschrieben von WOLFGANG UWE GROßMANN

Uwe Großmann