DATENSCHUTZ e.V.

Leitlinie zur Informationssicherheit

-Öffentlich-

Stand: November 2019

Betreuer des Dokuments	**Erich Hübner**	**Vorstand**
Freigabe	**Erich Hübner**	**Vorstand**
Revision	**21.09.2020**	

Aktuelle Version	Datum	Bearbeitet von	Freigabe
V1	21.09.2019	Erich Hübner	Erich Hübner

Leitlinie zur Informationssicherheit

Die Leitung verabschiedet hiermit folgende Leitlinie zur Informationssicherheit als Bestandteil ihrer Strategie:

Stellenwert der Informationsverarbeitung

Informationsverarbeitung spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf unser Geschäft nicht zusammenbrechen.

Übergreifende Ziele

Unsere Daten und unsere IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau. Für Daten der Entwicklungsabteilung gelten maximale Anforderungen an die Vertraulichkeit.

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

Alle Mitarbeiter und Mitglieder des **Datenschutz e.V.** halten die einschlägigen Gesetze und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für den Verein sowie für die Mitarbeiter/ Mitglieder durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter/ Mitglieder und die Vereinsführung sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

Detailziele

Verspätete oder fehlerhafte Entscheidungen der Leitung können weitreichende Folgen nach sich ziehen. Daher ist für die Leitung bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicher zu stellen.

Die Datenschutzgesetze und die Interessen unserer Mitarbeiter/ Mitglieder verlangen eine Sicherstellung der Vertraulichkeit der Daten. Die Daten und die IT-Anwendungen der Personalabteilung werden daher einem hohen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Kunden und Geschäftspartner.

Für die Vertriebs- Marketingabteilung ist die Aufrechterhaltung der Kommunikation nach außen zu den Kunden und Geschäftspartnern und der Zugriff auf die Kundendatenbank elementar. Die Geschäftsabwicklung darf nicht verzögert oder gar gefährdet werden. Wenn vertraglich festgelegte Lieferfristen nicht eingehalten werden können, kann dies weitreichende negative Folgen haben. Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu Erlösminderungen führen. Die Aufrechterhaltung der Kommunikation und der ständige Zugriff auf korrekte Daten für die Mitarbeiter/ Mitglieder hat einen hohen Schutzbedarf.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch

entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Informationssicherheitsmanagement

Zur Erreichung der Informationssicherheitsziele wird eine Sicherheitsorganisation eingerichtet. Es wird ein IT-Sicherheitsbeauftragter benannt werden. Der IT-Sicherheitsbeauftragte berichtet in seiner Funktion direkt an die Leitung. Dem IT-Sicherheitsbeauftragten und den Administratoren werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die von der Leitung festgelegten Informationssicherheitsziele zu erreichen.

Die Administratoren und der IT-Sicherheitsbeauftragte sind durch die IT-Benutzer ausreichend in ihrer Arbeit zu unterstützen.

Der IT-Sicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Die IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des IT-Sicherheitsbeauftragten zu halten.

Der Datenschutzbeauftragte hat ein ausreichend bemessenes Zeitbudget für die Erfüllung seiner Pflichten zur Verfügung. Der Datenschutzbeauftragte ist angehalten, sich regelmäßig weiterzubilden.

Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden.

Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden von uns konkrete Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Das Recht auf Kontrolle wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben erstellen wir ein detailliertes Sicherheitskonzept mit konkreten Maßnahmenvorgaben.

IT-Benutzer nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Leitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Verbesserung der Sicherheit

Das Managementsystem der Informationssicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern/ Mitglieder bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Leitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter/ Mitglieder 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 Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

München, 21.09. 2019

Vorstand. Dipl.-Ing. Erich Hübner