ND A.5.1 Informationssicherheitsrichtlinie

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

Stellenwert der Informationsverarbeitung

Informationsverarbeitung unterstützt unsere Aufgabenerfüllung und spielt eine wesentliche Rolle. Alle wesentlichen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt.

Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Da unsere Kernkompetenz in der Entwicklung und im Betrieb von Anwendungsprogrammen für unsere Kunden liegt, Ver- und Bearbeiten wir vielfach sensible Daten unserer Kunden. Der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung ist von existenzieller Bedeutung.

Übergreifende Ziele

Unsere Daten sowie die Daten unserer Kunden und unsere IT-Systeme in allen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können und keine wesentlichen Auswirkungen auf den Geschäftsbetrieb haben. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel, die Gewährleistung der Integrität ist ein wichtiges Ziel. Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau.

Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit Existenz bedrohenden finanziellen Auswirkungen (d. h. Auswirkungen von über 100% des monatlichen Umsatzes) müssen verhindert werden.

Alle Mitarbeiter des Unternehmens halten die einschlägigen Gesetze (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen sowie internen Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter und die Institutsleitung sind sich ihrer Verantwortung beim Umgang mit Informationen bewusst und unterstützen die Strategie zur Informationssicherheit nach besten Kräften.

Detailziele

Die Datenschutzgesetze und die Interessen unserer Mitarbeiter verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. Die Daten und die Anwendungen der Personalabteilung werden daher einem normalen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten unserer Kunden und Geschäftspartner.

Die Geschäftsabwicklung darf nicht verzögert oder gar gefährdet werden. Wenn vertraglich festgelegte Lieferfristen nicht eingehalten werden können, kann dies weit reichende negative Folgen haben. Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und der Daten, aber auch Fehlfunktionen können zu Erlösminderungen führen und Vertragsstrafen nach sich ziehen.

Innerhalb der Entwicklungsabteilung wird die Verfügbarkeit und die Fehlerfreiheit der Systeme sichergestellt. Ausfallzeiten von IT-Systemen innerhalb der Entwicklung sind nur in einem geringen Maße akzeptabel, da diese direkt, aber auch indirekt – durch negative Auswirkungen auf nachfolgende Prozesse – zu Erlösminderungen führen können.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich und für die Kommunikation mit Kunden und Geschäftspartnern wesentlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Sicherheitsmanagement

Zur Erreichung der Sicherheitsziele wurde ein IT-Sicherheitsbeauftragter benannt. Der IT-Sicherheitsbeauftragte ist für die Erstellung und Fortschreibung des Sicherheitskonzepts sowie die Aufrechterhaltung des Sicherheitsniveaus verantwortlich. Er berichtet in seiner Funktion direkt an die Geschäftsführung.

Dem IT-Sicherheitsbeauftragten werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen für die Ausübung seiner Tätigkeit zur Verfügung gestellt. Er ist durch die Verantwortlichen und Nutzer ausreichend zu unterstützen und frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Gleiches gilt, sofern personenbezogene Daten betroffen sind.

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

Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, 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 angemessenes 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 Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten den IT-Sicherheitsbeauftragten.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine Datensicherung wird daher gewährleistet, dass kurzfristig verlorene oder fehlerhafte Teile des operativen Datenbestandes wiederhergestellt werden können. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Benutzer nehmen mindestens jährlich an einer internen Sicherheitsunterweisung durch den IT-Sicherheitsbeauftragten teil.

Verbesserung der Sicherheit

Das Sicherheitskonzept wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft und bei Bedarf angepasst. Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an den IT-Sicherheitsbeauftragten 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 Sicherheitstechnik zu halten.

Für alle Themen, die in den Controls geregelt sind, hat der Inhalt Richtliniencharakter. Der Inhalt der Spalte Maßnahmen in grüner Schrift beinhaltet die Richtlinien, die einzuhalten sind.

Als übergreifender, nicht unternehmensspezifischer Leitfaden gilt das Dokument “DATEV_Leitfaden_Infosich_Mitarbeiter.pdf”