KACO Informations- und Datenschutzsicherheitsrichtlinie

Vorwort

Als einer der weltweit führenden Entwickler und Hersteller von hochpräzisen, anwendungsorientierten Dichtungslösungen für die Automobil- und Maschinenbauindustrie zeichnet sich KACO durch eine ausgeprägte Werkstoff- und Systemkompetenz und hohe Innovationskraft aus. Aus diesem Grund ist der Schutz unserer vertraulichen Daten sowie der Schutz vertraulicher Daten unserer Kunden von zentraler Bedeutung.

Die verlässliche Verfügbarkeit unserer IT- und Kommunikationssysteme ist entscheidend für einen reibungslosen Arbeitsablauf und die Verfügbarkeit von Daten.

Im Speziellen ist folgendes zu beachten:

Stellenwert der Informations- und Kommunikationstechnologien

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. Die Funktionsfähigkeit jedes Teilbereichs muss gewahrt sein. Da unsere Kernkompetenz in der Entwicklung innovativer Produkte liegt, ist der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von existenzieller Bedeutung. Gleiche Bedeutung messen wir auch dem Schutz personenbezogener Daten zu.

Übergreifende Ziele

Unsere Daten und unsere IT-Systeme in allen technischen und kaufmännischen Bereichen werden in ihrer **Verfügbarkeit** so gesichert, dass die zu erwartenden Stillstandszeiten auf ein tolerierbares Mindestmaß reduziert werden. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind soweit wie möglich zu vermeiden und nur in Ausnahmefällen akzeptabel **(Integrität).** Die Anforderungen an **Vertraulichkeit** orientieren sich am hohen Niveau der geltenden Gesetze. Für sensible personenbezogene Daten, Entwicklungs- oder Produktionsdaten gelten höchste Anforderungen an die Vertraulichkeit.

Die Standard-Sicherheitsmaßnahmen müssen zum Schutz der betroffenen Informationen geeignet sein und darüber hinaus in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Finanzielle Schäden aufgrund mangelnder IT-Sicherheit oder hohen Risiken für die persönlichen Rechte und Freiheiten von Personen müssen verhindert werden.

Alle Mitarbeiter des Unternehmens halten die einschlägigen Gesetze (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen Regelungen ein. Allen Mitarbeitern ist bewusst, dass im Falle eines Gesetzesverstoßes schwerwiegende finanzielle und immaterielle Konsequenzen für das Unternehmen sowie für die verantwortlichen Personen drohen. Jegliche Nichterfüllung der Pflichten wird verfolgt und geahndet, Verstöße ziehen Disziplinarmaßnahmen nach sich die abhängig von dem Schweregrad des Verstoßes bis hin zur außerordentlichen Kündigung führen können.

Alle Mitarbeiter und die Unternehmensführung sind sich ihrer Verantwortung beim Umgang mit den Informations- und Kommunikationstechnologien bewusst und unterstützen die Sicherheitsstrategien nach besten Kräften.

Detailziele

Verspätete oder fehlerhafte Managemententscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für das Management 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 verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. 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 Vertriebsabteilung 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. 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 Vertriebsmitarbeiter haben einen hohen Schutzbedarf.

Die Daten der Forschungs- und Entwicklungsabteilung unterliegen sehr hohen Vertraulichkeitsanforderungen. Deren Verlust, Veränderungen oder Diebstahl kann Wettbewerbsnachteile bedeuten. Durch technische Maßnahmen und die hohe Aufmerksamkeit der Mitarbeiter wird die Vertraulichkeit geschützt und Manipulationen vorgebeugt.

Innerhalb der Produktionsabteilung werden die Verfügbarkeit und die Fehlerfreiheit der Systeme sichergestellt da diese sich sowohl negativ auf die Produktqualität auswirken als auch zu Stillstandzeiten führen können uns damit die nachfolgenden Prozesse und letztendlich auch auf die Erlöse beeinträchtigen. Ausfälle sind daher soweit wie möglich zu vermeiden.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Büro-kommunikationswegen. Durch entsprechende Maßnahmen werden die Risiken der Internetnutzung stetig reduziert.

Informationssicherheits- und Datenschutzmanagement

Zur Erreichung der Informationssicherheits- und Datenschutzziele wurde eine Sicherheitsorganisation eingerichtet. Es sind IT-Sicherheits- und Datenschutzbeauftragte benannt worden. Die Beauftragten berichtet in ihrer Funktion direkt an die Geschäftsleitung.

Den Beauftragten und den Administratoren werden von der Geschäftsleitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die von der Geschäftsleitung festgelegten Informationssicherheits- und Datenschutzziele zu erreichen.

Die Administratoren und die Beauftragte 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-Sicherheitsbeauftragen bzw. des Datenschutzbeauftragten zu halten.

Sicherheitsmaßnahmen

Für alle Verfahren, Daten, Informationen, IT-Anwendungen und IT-Systeme sind verantwortliche Personen benannt, die dem jeweiligen Schutzbedarf, der in einem funktionsübergreifenden Team bestimmt wurde, entsprechend Zugriffsberechtigungen vergeben.

Für alle verantwortlichen Funktionen sind Vertretungen benannt.

Gebäude und Räumlichkeiten werden durch geeignete Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen beschränkt. Ein restriktives Berechtigungskonzept regelt den Zugriff auf die Daten.

Computer-Viren-Schutzprogramme werden in allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Die Schutzprogramme sind so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Die IT-Benutzer sind aufgefordert, diese Sicherheitsmaßnahmen durch eine sicherheitsbewusste Arbeitsweise zu unterstützen und bei Auffälligkeiten die entsprechend festgelegten Stellen zu informieren.

Trotz aller Sicherheitsmaßnahmen können Datenverluste nie vollkommen ausgeschlossen werden. In einem solchen Fall wird durch eine umfassende Datensicherung gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen und Daten 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, geben wir konkrete Sicherheitsanforderungen in den Service Level Agreements vor. Zudem behalten wir uns Kontrollrechte vor. Für umfangreiche oder komplexe Outsourcing-Vorhaben erstellen wir ein detailliertes Sicherheitskonzept mit konkreten Maßnahmenvorgaben.

Die Regelungen zur Informationssicherheit und zum Datenschutz sind für alle Mitarbeiter im Intranet verfügbar und werden regelmäßig in Schulungen vermittelt. Für alle IT-Benutzer werden regelmäßig Schulungen zur korrekten Nutzung von Informations- und Kommunikationstechnologien und den hiermit verbundenen Sicherheitsmaßnahmen durchgeführt. Die Geschäftsleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Verbesserung der Sicherheit

Das Managementsystem wird regelmäßig auf seine Aktualität und Wirksamkeit hin überprüft. Daneben werden die Sicherheitsmaßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Geschäftsleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungsvorschläge oder Hinweise auf 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.

KACO Information and Privacy Security Policy

Foreword

As one of the world's leading developers and manufacturers of high-precision, application-oriented sealing solutions for the automotive and mechanical engineering industries, KACO is distinguished by its outstanding materials and systems expertise and innovative strength. For this reason, the protection of our confidential data and the protection of confidential data of our customers is of crutial importance.

The reliable availability of our IT and communications systems is significant to ensure a smooth workflow and availability of data.

In particular, the following should be noted:

The importance of information and communication technologies

Information processing plays a key role in the fulfillment of our tasks. All key strategic and operational functions and tasks are significantly supported by information technology (IT). It must be possible to compensate for a failure of IT systems at short notice. The functionality of each subarea must be maintained. Since our core competence lies in the development of innovative products, the protection of this information against unauthorized access and unauthorized modification is of existential importance. We also attach the same importance to the protection of personal data.

Overarching goals

The availability of our data and our IT systems in all technical and commercial areas is secured in such a way that the expected downtimes are reduced to a tolerable minimum. Malfunctions and irregularities in data and IT systems shall be avoided as far as possible and are only acceptable in exceptional cases **(integrity). The confidentiality** requirements are based on the high level of the applicable laws**.** Highest confidentiality requirements apply to sensitive personal data, development or production data.

The standard security measures must be suitable for the protection of the information concerned and, moreover, must be in an economically justifiable relation to the value of the information and IT systems requiring protection. Financial damage due to lack of IT security or high risks to the personal rights and freedoms of persons must be prevented.

All employees of the Company comply with applicable laws (e.g. Criminal Code, Industrial Constitution Act, Commercial Code, Social Code, laws and regulations on data protection) and contractual provisions. All employees are aware that in the event of a legal offence there are serious financial and immaterial consequences for the company and the responsible persons. Any non-fulfillment of duties will be taken seriously and prosecuted, violations will result in disciplinary action which, depending on the severity of the violation, may lead to extraordinary termination.

All employees and management are aware of their responsibility in dealing with information and communication technologies and support the security strategies to the best of their ability.

Detailed goals

Late or incorrect management decisions can have far-reaching consequences. This is why it is important for management to have access to current control data when making important decisions. A high level of security in terms of availability and integrity shall be ensured for this information.

The data protection laws and the interests of our employees require us to ensure the confidentiality of employee data. The data and IT applications of the Human Resources Department are therefore subject to a high level of confidentiality protection. The same applies to the data of our customers and business partners.

Maintaining external communication with customers and business partners and access to the customer database is essential for the Sales Department. Business transactions must not be delayed or even jeopardized. In particular, poor availability of IT systems and data, but also malfunctions, can lead to revenue reductions. The maintenance of communication and the constant access to correct data for the sales staff have a high need for protection.

The data of the research and Development Department are subject to very high confidentiality requirements. Their loss, alteration or theft can result in competitive disadvantages. Technical measures and the high attention of the employees protect confidentiality and prevent manipulation.

Within the Production Department, the availability and faultlessness of the systems are ensured as these can have a negative impact on product quality as well as lead to downtimes which can affect subsequent processes and, ultimately, the revenues. Failures shall be avoided as far as possible.

It goes without saying that we use the Internet to obtain information and to communicate. E-mail serves as a substitute or supplement for other office communication channels. Appropriate measures are taken to reduce the risks of internet use steadily.

Information security and data protection management

A security organization has been set up to achieve the information security and data protection objectives. IT security and data protection officers have been appointed. In their function, the representatives report directly to the General Management.

General Management shall provide sufficient financial and time resources to the delegates and administrators to enable them to receive regular training and information and to achieve the information security and data protection objectives set by General Management.

The administrators and the representative shall be adequately supported in their work by the IT users.

The IT security officer must be involved in all projects at an early stage in order to consider security-relevant aspects already in the planning phase. If personal data are concerned, the same applies to the data protection officer.

The IT users have to follow the instructions of the IT security officer or the data protection officer in security-relevant questions.

Safety precautions

Responsible persons are appointed for all procedures, data, information, IT applications and IT systems, who assign access authorizations according to the respective protection requirements determined in a cross-functional team.

Representatives are appointed for all responsible functions.

Buildings and premises are protected by appropriate access controls. Access to IT systems is protected by appropriate access controls either. A restrictive authorization concept regulates the access to data.

Computer virus protection programs are used on all IT systems. All Internet access is secured by a suitable firewall. The protection programs are configured and administered to provide effective protection and prevent tampering. IT users are encouraged to support these security measures by a safety-conscious operation and to inform the correspondingly defined locations in the event of anomalies.

Despite all security measures, data losses can never be completely ruled out. In such a case a comprehensive data backup ensures that IT operations can be resumed at short notice if parts of the operative data stock are lost or are obviously faulty. Information and data are marked uniformly and stored in such a way that they can be found quickly.

In order to limit or prevent major damage as a result of emergencies, security incidents must be dealt with promptly and consistently. Emergency measures are compiled in a separate emergency

precaution concept. Our goal is to maintain critical business processes even in the event of a system failure and to restore the availability of the failed systems within a tolerable period of time.

If IT services are outsourced to external parties, we stipulate specific security requirements in the Service Level Agreements. In addition, we reserve the right to control. For extensive or complex outsourcing projects, we create a detailed security concept with concrete measures.

The regulations on information security and data protection are available to all employees on the Intranet and are regularly taught in training courses. Training courses on the correct use of information and communication technologies and the associated security measures are carried out regularly to all IT users. The management supports the need-based further education and training.

Safety improvement

The management system is regularly checked for its topicality and effectiveness. In addition, the safety measures are regularly examined to determine whether they are known to the employees concerned, whether they can be implemented and whether they can be integrated into the operating procedure.

The General Management supports the continuous improvement of the safety level. Employees are encouraged to pass on possible improvement suggestions or indications of weaknesses to the appropriate departments.

The desired level of security and data protection is ensured through continuous revision of the regulations and their compliance. Deviations are analyzed with the aim of improving the security situation and keeping it constantly up to date with the latest IT security technology.

KACO 信息和数据保护安全政策

前言

作为汽车和机械工程行业内以应用为导向的高精度密封解决方案的全球领先的开发商和制造商之一，KACO 公司凭借其卓越的原材料和系统技能以及雄厚的创新实力而出众。因此，保护我们的机密信息和客户的机密信息至关重要。

IT 和通信系统的可靠的可用性对于确保流畅的工作流程和数据可用性至关重要。

尤其需要注意以下几点：

信息和通信技术的重要性

信息处理在我们的任务执行中起着关键作用。信息技术（IT）显著支持着所有基本的战略和运营的功能与任务。IT 系统的故障必须能够在短期内整体得到弥补。必须保留每个分区的功能作用。由于我们的核心能力在于创新产品的开发，因此保护这些信息免遭未经授权的访问和未经授权的修改至关重要。我们也同样重视个人数据的保护。

全面的目标

我们确保在所有技术和商业领域的数据和 IT 系统的**可用性**，从而将预期的停机时间减少到可以容忍的最低限度。应尽可能避免数据和 IT 系统中的故障和违规行为，并且只有在特殊情况下才可以接受（**完整性**）。**机密性**的要求针对于高度适用的法律法规。对于敏感的个人数据，开发或生产数据，最高机密性要求是适用的。

标准安全措施必须适用于对相关信息的保护，此外它还必须与需要保护的信息和 IT 系统的价值存在经济上合理的关系。必须防止由于缺乏 IT 安全性或关于人身权利和自由的高风险而造成的财务损失。

公司所有员工都需遵守相关法律（例如刑法，企业章程法，商业法，社会法，数据保护法律法规）和合同条款。所有员工都应了解，如果违反法律，将会给公司和相关责任人带来严重的财务和非物质后果。任何不履行职责的行为都将被追究和处罚，违规行为将视情况而定、根据违规的严重程度给予纪律处分，甚至可能会被特殊解雇。

所有员工和公司管理层都必须意识到他们在处理信息和通信技术方面的责任，并尽其所能支持安全战略。

具体目标

延迟的或不正确的管理决策可能会产生深远的影响。因此，访问最新的控制数据对于管理的重要决策至关重要。在可用性和完整性方面，这些信息需要高度的安全性。

数据保护法和我们员工的利益要求对员工数据保密。因此，人事部门的数据和 IT 应用程序受到高度保密。这同样适用于我们的客户和业务合作伙伴的数据。

维持与客户和业务合作伙伴的外部通信以及访问客户数据库对于销售部门至关重要。经营业务不得延误甚至受到危害。特别是缺乏 IT 系统和数据的可用性，并且功能故障还会导致收入减少。对于销售人员而言，维护通信和不断访问正确的数据具有很高的保护需求。

研发部门的数据具有很高的机密性要求。它们的丢失、改动或被盗可能导致竞争劣势。通过技术措施和高度的员工关注度，可以保护机密信息并防止对其进行操纵。

在生产部门内，需确保系统的可用性和无缺陷性，因为它们会对产品质量产生负面影响，并导致停机，从而损害后续流程和最终的收入。因此应尽可能避免故障。

对于我们来说使用互联网获取信息和进行交流是理所当然的。电子邮件可以替代或补充其他办公室通信渠道。通过适当的措施，互联网使用的风险被持续降低。

信息安全与数据保护管理

为了满足信息安全和数据保护目标，我们成立了一个安全组织。已任命了 IT 安全和数据保护专员。专员直接向管理层汇报他的职务。

管理层给专员和行政管理人员提供足够的财务和时间资源，以定期进行自我深造和报告，并实现管理层设定的信息安全和数据保护目标。

行政人员和专员在他们的工作中得到了 IT 用户足够的支持。

IT 安全专员必须尽早参与所有项目，以便在计划阶段考虑到与安全相关的方面。如果涉及个人数据，则同样适用于数据保护专员。

对于与安全相关的问题，IT 用户必须遵循 IT 安全专员或数据保专员的要求。

安全措施

对于所有程序、数据、信息、IT 应用和 IT 系统应指定负责人，授予这些负责人相应的由跨职能的团队所确定的保护要求的访问权限。

所有相应的职能需指定代理。

建筑物和场所会受到适当的访问控制的保护。对 IT 系统的访问受到适当的访问控制的限制。限制性的校正计划可处理对数据的访问。

所有 IT 系统都使用计算机病毒防护程序。所有网络访问均由合适的防火墙保护。配置和管理这些保护程序的方式应使其提供有效的保护并防止被操纵。要求 IT 用户通过一种注重安全的工作方式来支持这些安全措施，并在出现异常情况时通知他们。

即使采取所有安全措施也永远不可能完全排除数据的丢失。在这种情况下，全面的数据备份可确保在部分运营数据丢失或明显出现故障时，可以在短时间内恢复 IT 运营。信息和数据被统一标识并存储，以便于快速检索。

为了限制或防止由于紧急情况而造成的重大损失，必须迅速而持续地处理安全事件。应急措施建立在单独的应急预防计划中。我们的目标是即使在系统出现故障的情况下也能维持关键的业务流程，并在可容忍的时间内恢复故障系统的可用性。

如果将 IT 服务外包给外部的单位，我们将在服务等级协议中给出特定的安全要求。此外，我们需保留控制权。对于大型或复杂的外包项目，我们会创建带有具体措施规定的详细的安全计划。

Intranet 上的有关信息安全和数据保护的法规对于所有员工均是适用的，并且会定期在培训中介绍。定期为所有 IT 用户提供正确使用信息和通信技术以及相关安全措施的培训。管理层支持所有需求相关的学习和培训。

安全性改善

定期检查管理系统的及时性和有效性。此外，定期检查安全措施，以确定相关员工是否知道这些安全措施，是否可以实施这些措施并将其融入到工作过程中。

管理层支持着安全级别的不断提高。员工被要求将可能的改进建议或缺陷说明传达给有关部门。

通过不断修订和遵守规定可以确保所需要的安全性和数据保护的水平。分析与目标的偏差来改善安全状况并使其与 IT 安全技术现有状态保持一致。

KACO Információs és adatvédelmi irányelv

Előszó

Az autó- és gépgyártási iparág számára kiválóan illeszkedő, a felhasználás igényeinek megfelelő tömítési megoldások világszerte vezető fejlesztőjeként és gyártójaként a KACO kiforrott alapanyag- és rendszer-kompetenciával és magas innovációs erővel tűnik ki. Ezen oknál fogva saját bizalmas adataink, és ügyfeleink bizalmas adatainak védelme központi jelentőséggel bír.

IT- és kommunikációs rendszereink megbízható rendelkezésre állása döntő fontosságú a zavartalan munkafolyamatokhoz és az adatok elérhetőségéhez.

Részleteiben a következőket kell figyelembe venni:

Az információs és kommunikációs technológiák helye és értéke

Az információk feldolgozása feladataink teljesítésében kulcsfontosságú szerepet játszik. Az információs-technológia (IT) minden lényeges stratégiai és operatív funkciót és feladatot jelentős mértékben támogat. Az IT-rendszerek kiesését összességében rövid időn belül tudni kell kompenzálni. Minden rendszer működőképességének biztosítottnak kell lennie. Mivel központi kompetenciánkat az innovatív termékek fejlesztése képezi, ezeknek az információknak jogosulatlan hozzáférés és tiltott módosítás ellen történő védelme létfontosságú. Ugyanilyen jelentőséget tulajdonítunk a személyes adatok védelmének is.

Célok átfogóan

Adataink és IT-rendszerünk **rendelkezésre állása** minden műszaki és kereskedelmi területen úgy van biztosítva, hogy az elvárt állásidők egy tűrhető minimum mértékre redukálódjanak. Az adatokban és IT-rendszerekben fellépő hibákat és rendszertelenségeket amennyire lehet, kerülni kell, ezek csak kivételes esetekben elfogadhatóak **(integritás).** A **titoktartással** szemben támasztott követelmények az érvényes törvények magas színvonalához igazodnak. Érzékeny személyes adatokra, a fejlesztési és gyártási adatokra a bizalmasság legmagasabb követelményei érvényesek.

A standard biztonsági intézkedéseknek alkalmasnak kell lenniük az érintett információk védelmére, és ezen felül gazdaságilag vállalható arányban kell állniuk a védendő információk és IT-rendszerek értékével. Hiányos IT-biztonság miatti anyagi károkat vagy a személyek személyes jogai és szabadságai sérülésének magas kockázatát meg kell akadályozni.

A vállalat minden dolgozója betartja az idevágó törvényeket (pl. büntető törvénykönyv, üzemi alaptörvény, kereskedelmi törvénykönyv, társadalombiztosítási törvénykönyv, adatvédelmi törvények és rendeletek) és a szerződéses szabályozásokat. Minden munkatárs tudatában van annak, hogy a törvények megszegése súlyos pénzbeli és nem pénzbeli következményekkel járhat a vállalat, valamint a felelős személyek számára. A bármely kötelezettség nem teljesítése kivizsgálást és büntető eljárást von maga után, a vétségek fegyelmi eljárást vonnak maguk után, mely a vétség súlyosságától függően akár felmondáshoz is vezethet.

Minden munkatárs és a vállalat vezetése is tudatában van felelősségének az információs- és kommunikációs technológiák kezelése során, és a biztonsági stratégiákat legjobb tudása szerint támogatja.

Célok részletezve

Egy megkésett vagy hibás menedzsment-döntésnek messzire nyúló következménye lehet. Ezért a fontos döntésekhez a menedzsment számára lényeges az aktuális irányítási adatokhoz való hozzáférés. Ezeknél az információknál biztosítani kell a rendelkezésre állás és az integritás magas biztonsági színvonalát.

Az adatvédelmi törvények és munkatársaink érdekei megkövetelik a munkatársi adatok bizalmasságának biztosítását. A személyi osztályon található adatok és IT-alkalmazások

különlegesen magas biztonsági védelem alá esnek. Ugyanez érvényes ügyfeleink és üzleti partnereink adataira.

Az értékesítés számára a kívülre, az ügyfelekkel és üzleti partnerekkel történő kommunikáció és az ügyfél-adatbankhoz történő hozzáférés alapvetően szükséges. Az üzleti folyamatok lebonyolítása nem késlekedhet, főleg nem kerülhet veszélybe. Különösen az IT-rendszerek és adatok hiányos rendelkezésre állása, de hibás működés is bevételkieséshez vezethet. A kommunikáció és a megfelelő adatokhoz történő hozzáférés fenntartása az értékesítési munkatársak számára fontos adatvédelmi igény.

A kutatási és fejlesztési részleg adatai különösen magas titoktartási követelmények alá tartoznak. Ezek elvesztése, módosítása vagy ellopása a konkurenciával szemben hátrányt jelenthet. Műszaki intézkedésekkel és a munkatársak nagyfokú odafigyelésével a bizalmasságot védeni kell, a manipulációt pedig meg kell előzni.

A termelési részlegen belül biztosítani kell a rendszerek rendelkezésre állását és hibamentességét, mivel ezek hiánya egyrészt negatívan hathat ki a termékminőségre, másrészt leállási időkhöz vezethet, ami által a következő folyamatok végeredményben az árbevételt is negatívan befolyásolják. A kieséseket ezért amennyire csak lehet, kerülni kell.

Az internet használata információk beszerzésére és kommunikációra számunkra magától értetődő. Az e-mail helyettesíti, vagy kiegészíti a többi irodai kommunikációs útvonalat. Megfelelő intézkedésekkel az internethasználat kockázatát állandóan csökkenteni kell.

Információs biztonsági és adatvédelmi irányítás

Az információs biztonsági és adatvédelmi célok eléréséhez biztonsági szervezetet működtetünk. Kineveztük az IT-biztonsági és adatvédelmi megbízottakat. A megbízottak ilyen funkciójukban közvetlenül az ügyvezetésnek jelentenek.

Az ügyvezetés elegendő pénzügyi és időforrást bocsát a megbízottak és adminisztrátorok rendelkezésére, hogy rendszeresen tovább tudják képezni magukat, illetve tájékozódni tudjanak, és elérjék az ügyvezetés által meghatározott információs biztonsági és adatvédelmi célokat.

Az adminisztrátorokat és megbízottak munkáját az IT-felhasználóknak megfelelően támogatniuk kell.

Az IT-biztonsági megbízottat időben be kell vonni minden projektbe annak érdekében, hogy már a tervezési szakaszban figyelembe vegyék a biztonsági szempontból fontos aspektusokat. Amennyiben személyes adatok érintettek, akkor ugyanez érvényes az adatvédelmi megbízottra.

Az IT-felhasználóknak biztonsági szempontból fontos kérdések esetén tartaniuk kell magukat az IT-biztonsági megbízott, ill. az adatvédelmi megbízott utasításaihoz.

Biztonsági intézkedések

Minden eljárásra, adatra, információra, IT-alkalmazásra és IT-rendszerre felelős személyeket neveztünk ki, akik egy funkciókat átfogó team által meghatározott mindenkori védelmi szükségletnek megfelelően hozzáférési jogosultságokat adnak meg.

Minden felelős funkcióban van helyettes személy.

Az épületet és helyiségeket megfelelő beléptetési ellenőrzéssel védik. Az IT-rendszerekhez történő hozzáférést megfelelő hozzáférési ellenőrzés korlátozza. Egy tiltó jogosultsági koncepció szabályozza az adatokhoz történő hozzáférést.

Számítógépes vírusok elleni védőprogramokat minden IT-rendszerben használnak. Minden internetes hozzáférést megfelelő tűzfal biztosít. A védőprogramokat úgy konfigurálták és adminisztrálták, hogy azok hatékony védelmet jelentsenek, és megakadályozzák a manipulációt. Az IT-felhasználókat felszólítjuk, hogy biztonsági szempontból tudatos munkával támogassák ezeket a biztonsági intézkedéseket, és feltűnő események esetén megfelelően tájékoztassák a megadott helyeket.

Az adatvesztést minden biztonsági intézkedés ellenére sem lehet soha teljesen kizárni. Ilyen esetben átfogó adatbiztosítás garantálja, hogy az IT-üzemeltetést rövid határidőn belül ismét folytatni lehessen, ha az operatív adatállomány egyes részei elvesznek, vagy nyilvánvalóan hibásak. Az információkat és adatokat egységesen kell jelölni, és úgy kell megőrizni, hogy gyorsan ismét fellelhetőek legyenek.

Vészhelyzet esetén a károk korlátozása, illetve még nagyobb károk megelőzése érdekében a biztonsági eseményekre gyorsan és konzekvensen kell reagálni. A vészhelyzetben szükséges intézkedéseket egy külön vészhelyzet-megelőzési koncepcióban foglaltuk össze. Célunk az, hogy még rendszerkiesés esetén is fenn lehessen tartani a kritikus üzleti folyamatokat, és a kiesett rendszerek rendelkezésre állását tűrhető időhatáron belül ismét helyre lehessen állítani.

Amennyiben valamely IT-szolgáltatást külsős szolgáltatóhoz helyezünk ki, akkor konkrét biztonsági követelményeket írunk elő a szolgáltatás fokát leíró megállapodásban (Service Level Agreements). Ezen kívül fenntartjuk az ellenőrzési jogot. Az átfogó vagy komplex kihelyezési szándékhoz részletes biztonsági koncepciót készítünk konkrét intézkedési előírásokkal.

Az információs biztonságra és adatvédelemre vonatkozó szabályozások minden munkatárs számára rendelkezésre állnak a belső hálózaton (intranet), illetve azokat rendszeresen oktatják. Minden IT-felhasználó számára rendszeres oktatásokat végzünk az információs- és kommunikációs technológiák megfelelő használatáról, és az ezekkel összefüggő biztonsági intézkedésekről. Az ügyvezetés támogatja a jogos igénynek megfelelő továbbképzést.

A biztonság javítása

Az irányítási rendszert rendszeresen felülvizsgáljuk aktualitását és hatékonyságát illetően. Emellett a biztonsági intézkedéseket rendszeresen megvizsgáljuk arra vonatkozóan, hogy azokat az érintett munkatársak ismerik-e, hogy azok végrehajthatóak-e és az üzemi folyamatokba integrálhatóak-e.

Az ügyvezetés támogatja a biztonsági szint állandó javítását. A munkatársakat kérjük, hogy az esetleges jobbítási javaslataikat vagy a gyenge pontokra történő figyelem-felhívásukat adják tovább a megfelelő helyekre.

A szabályzatok folyamatos felülvizsgálatával és azok betartásával biztosítjuk a megcélzott biztonsági és adatvédelmi szintet. Az eltéréseket elemezzük abból a célból, hogy javítsuk a biztonsági állapotot, és azt az aktuális IT-biztonságtechnikai színvonalon tartsuk.