Managementsystemhandbuch

1 Managementsystemhandbuch Allgemein

Anlage 2 Sicherheitsleitlinie

Inhalt

1 Informationssicherheit im Bereich der Dresden-IT GmbH

1.1 Unternehmensvorstellung

Die Dresden-IT GmbH, im Weiteren als DD-IT bezeichnet, ist als Tochterunternehmen der Technischen Werke Dresden GmbH und der Dresdner Verkehrsbetriebe AG als kommunales Unternehmen in der IT-Branche seit 2002 tätig. Hauptziel dieser Neugründung war die Schaffung eines kompetenten IT-Dienstleisters für die Betriebe und Einrichtungen der Landeshauptstadt Dresden sowie für kommunale Partner in der Region.

Oberstes Ziel ist die Erbringung von qualitativ hochwertigen Dienstleistungen unter Einhaltung der gesetzlichen Forderungen. Die DD-IT ist seit November 2004 nach DIN EN ISO 9001 und seit November 2010 nach DIN ISO/IEC 27001 zertifiziert. Die Qualitätspolitik ist durch die Schwerpunkte Kundenzufriedenheit, Gewinnorientierung und Mitarbeiterzufriedenheit gekennzeichnet und die Sicherheitspolitik durch die Schwerpunkte Schutz von Informationen vor Bedrohungen, Aufrechterhaltung des Geschäftsbetriebes und Minimierung der Geschäftsrisiken.

Mit Ihrem Potenzial bei der Bereitstellung von IT-Servicedienstleistungen und Ihren Entwicklungs- und Beratungskapazitäten unterstützt die DD-IT Ihre Dienstleitungspartner bei der effektiven Gestaltung der IT-Prozesse.

Zur Erfüllung seiner Aufgaben arbeitet die DD-IT eng mit Dienstleitungspartnern zusammen und hat Kooperationen mit Einrichtungen der Landeshauptstadt Dresden sowie Partnern aus der Privatwirtschaft.

Die DD-IT setzt auf partnerschaftliche Zusammenarbeit sowie auf nationale und internationale Standards, Standards des Bundes und des Freistaates Sachsen.

1.2 Sicherheitserfordernisse

Auf der Grundlage des zertifizierten Qualitätsmanagementsystems (QMS) stehen die Erfüllung der Dienstleitungsverträge und aller damit verbundenen Leistungen im Mittelpunkt der täglichen Arbeit. Für alle Leistungen wird aufbauend auf dem Informationssicherheitsmanagementsystem (ISMS) ein hohes Maß an Qualität und Sicherheit vorgegeben und umgesetzt.

Informationen in jeglicher Form, elektronisch gespeichert oder elektronisch übertragen, auf Papier ausgedruckt oder geschrieben, oder in Gesprächen weitergegeben sind unabhängig von der gewählten Form, dem Medium der Weitergabe oder der Speicherung immer angemessen zu schützen.

Der Schutz von Informationen vor Bedrohungen, die Aufrechterhaltung des Geschäftsbetriebes und eine Minimierung der Geschäftsrisiken sind Elemente der Informationssicherheit.

Die Informationssicherheit stellt einen entscheidenden Faktor dar, um relevante Risiken zu vermeiden oder zu reduzieren.

Die Definition, das Erreichen, die Pflege und ständige Verbesserung von Informationssicherheit kann wesentlich zur Erhaltung von Wettbewerbsfähigkeit, Liquidität, Rentabilität, Einhaltung gesetzlicher Vorschriften und Geschäftsansehen beitragen.

Geeignete Maßnahmen, die Richtlinien, Prozesse, Technische Standards, Organisationsstrukturen oder Software- und Hardwarefunktionen sein können, dienen der Umsetzung der Informationssicherheit.

Diese Maßnahmen müssen eingeführt, umgesetzt, überwacht, überprüft und ständig verbessert werden, um sicherzustellen, dass die spezifischen Sicherheits- und Geschäftsziele der DD-IT und ihrer Dienstleistungspartner und Kunden erfüllt werden. Dies sollte im Einklang mit allen anderen Managementprozessen geschehen.

Unsere Auftraggeber haben die Möglichkeit, sich in die Weiterentwicklung der Informationssicherheit einzubringen, um so bei der dauerhaften kontinuierlichen Verbesserung mitzuwirken.

Als IT-Dienstleister werden bei der DD-IT auch personenbezogene Daten im wesentlichen Umfang gespeichert und verarbeitet. Daran sind die Sicherheitsanforderungen bei der DD-IT auszurichten.

Durch eine methodische Betrachtung und Einschätzung von Sicherheitsrisiken werden Sicherheitsanforderungen ermittelt, mittels Risikosteckbriefen bewertet und innerhalb des Risikomanagements Maßnahmen ergriffen um die Sicherheitsrisiken zu minimieren.

1.3 Sicherheit als Unternehmensziel

Sicherheit als wichtiger Baustein einer dauerhaft gut funktionierenden Organisation ist somit ein permanentes Unternehmensziel der DD-IT. Daraus ergibt sich ein stets vorhandenes Sicherheitsbewusstsein bei allen Arbeiten. Jeder Mitarbeiter wirkt mit, das Sicherheitsniveau und die damit verbundenen Methoden und Prozesse dauerhaft zu verbessern sowie die Geschäftstüchtigkeit im Notfall aufrecht zu erhalten.

Das Ziel ist es, mit einem an die Erfordernisse angepassten ISMS ein vertrauenswürdiges Sicherheitsniveau dauerhaft aufrecht zu erhalten.

2 Grundsatz

2.1 Orientierung

Der zuverlässige Schutz von Informationen ist notwendig auf Grund von:

- internationalen und nationalen Standards und Richtlinien,
- gesetzlichen Anforderungen, zum Beispiel Datenschutzgesetz und Steuerrecht,
- vertraglichen Anforderungen.

Es sind daher Maßnahmen zu treffen, die die Funktionsfähigkeit der Geschäftsprozesse der DD-IT und deren Kunden gewährleisten und die Verfügbarkeit, Vertraulichkeit und Integrität der Daten sicherstellen. Bedrohungen, wie höhere Gewalt, technisches Versagen, Nachlässigkeit oder Fahrlässigkeit und Schwachstellen, welche das Eintreffen dieser Bedrohungen begünstigen, sollen aufgezeigt werden, um Schadensereignisse abzuwehren und so Schäden zu vermeiden.

Die Mitarbeiter der DD-IT und die Mitarbeiter unserer Kunden werden grundsätzlich als vertrauenswürdig angesehen. Ein vertrauensvolles und konstruktives Arbeitsklima, in dem Teamgeist

und Eigenverantwortung einen hohen Stellenwert besitzen, bildet die beste Grundlage für einen reibungslosen, sicheren und effektiven Gebrauch der Informationstechnik.

Ungeachtet des oben aufgestellten Vertrauensgrundsatzes ist es erforderlich, die Wirkungsbereiche auf technischer Ebene voneinander abzugrenzen. Damit sollen Fernwirkungen von Fehlfunktionen und Handlungen, die in den Bereich der Sabotage gehören sowie die Folgen eines Einbruchs Unbefugter in IT-Systeme bzw. in das Netz begrenzt werden.

Die IT-Sicherheitsleitlinie bezieht sich auf alle Aspekte des IT-Einsatzes und legt fest, welche Sicherheitsmaßnahmen zu treffen sind. Nur bei geordnetem Zusammenwirken von technischen, organisatorischen, personellen und baulichen Maßnahmen können drohende Gefahren erfolgreich abgewehrt und begünstigende Schwachstellen vermieden werden.

2.2 Klassifizierung und Kontrolle

Alle Informationen, Daten und Datensammlungen werden nach Verfügbarkeit, Vertraulichkeit und Integrität/Authentizität klassifiziert. Aufbauend auf dieser Klassifizierung werden die Verantwortungen für die folgenden Objekte definiert und bekannt gegeben:

- Systeme, Software
- Einzelne Abschnitte der Infrastruktur

Es ist definiert, wer Eigentümer der Objekte ist und damit die Verantwortung für deren Sicherheit trägt.

Die Aktualität der Klassifizierung und daraus abgeleiteter Maßnahmen wird durch regelmäßige Überprüfung aufrechterhalten.

2.3 Grundbegriffe der Sicherheitsleitlinie

Im Folgenden werden die zentralen Begriffe der Sicherheitsleitlinie der DD-IT erläutert.

Verfügbarkeit
Verfügbarkeit bezieht sich auf Daten und Verfahren und bedeutet, dass diese zeitgerecht zur Verfügung stehen.

Vertraulichkeit
Vertraulichkeit ist gewährleistet, wenn nur diejenigen von Daten Kenntnis nehmen können, die dazu berechtigt sind. Daten dürfen weder unbefugt gewonnen noch ungewollt offenbart werden.

Integrität
Integrität ist gewährleistet, wenn Daten unversehrt und vollständig bleiben.

Authentizität
Authentizität bedeutet, dass Daten jederzeit ihrem Ursprung zugeordnet werden können.

Revisionsfähigkeit
Revisionsfähigkeit bezieht sich auf die Organisation des Verfahrens. Sie ist gewährleistet, wenn Änderungen an Daten nachvollzogen werden können.

Transparenz
Transparenz ist gewährleistet, wenn das IT-Verfahren für die jeweils Sachkundigen in zumutbarer Zeit mit zumutbarem Aufwand nachvollziehbar ist. In der Regel setzt dies eine aktuelle und angemessene Dokumentation voraus.

Datenschutz
Datenschutz regelt die Verarbeitung personenbezogener Daten, um das Recht des Einzelnen zu schützen und selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

3 Methoden

3.1 Systemzugangskontrolle

Die DD-IT setzt logische und physische Zugangskontrollen für den Zugang zu Informationen, Daten und Datensammlungen ein. Für besonders schützenswerte Bereiche wird eine verstärkte Zugangskontrolle durchgeführt. Diese wird protokolliert, um die geschützten Bereiche nachvollziehbar zu überwachen. Die Verantwortung für die Zugangskontrollen und deren regelmäßige Dokumentation liegen bei den Verantwortlichen der jeweiligen Bereiche. Für Informationen, Daten und Datensammlungen sind Verantwortliche festgelegt, diese sind für ihre Verantwortungsbereiche rechenschaftspflichtig. Für jede zusätzlich eingerichtete Berechtigung wird der tatsächliche Geschäftsbedarf des Nutzers überprüft.

3.2 Redundanzen

Für die dauerhafte Aufrechterhaltung des Geschäftsbetriebes ist eine Redundanz an Systemen und Wissen vorhanden. Durch technische Maßnahmen wird gewährleistet, dass im Notfall der Geschäftsbetrieb aufrechterhalten wird. Unsere Mitarbeiterstruktur ist dabei so zusammengesetzt, dass bei Ausfall einzelner Mitarbeiter eine Wissensredundanz für besonders sensible Verfahren, Prozesse und Systeme vorhanden ist, um Projekte, Vorhaben und Kundenanforderungen weiterzuführen.

3.3 Sicherheit der Informationssysteme innerhalb des Lebenszyklus

Durch Festlegungen im ISMS sind die Prozesse definiert, die die Sicherheit der Informationssysteme im gesamten Lebenszyklus, angelehnt an ITIL, beschreiben. In der Geschäftstätigkeit der DD-IT ist das vorhandene Risikofrüherkennungssystem fest verankert und wird kontinuierlich an die Erfordernisse angepasst.

3.4 Verantwortlichkeiten

Besitzer der Informationen ist üblicherweise der Auftraggeber. Bei Übergabe der Daten an die DD-IT wird ein Verantwortlicher gemäß ISMS - Richtlinien und Organisationsstruktur festgelegt. Je größer die Schutzwürdigkeit von Daten eingestuft wurde, desto stärker ist der Absicherungsprozess.

3.5 Bewusstsein

Die DD-IT stellt sicher, dass alle neuen Mitarbeiter mit der Sicherheitsleitlinie, den ISMS-Dokumenten und der Philosophie der DD-IT durch Schulungen vertraut gemacht werden. Den Dienstleistungs- und Kooperationspartnern, Beratern und Zulieferern wird die Sicherheitsleitlinie zur Verfügung gestellt. Der Sicherheitsprozess und die Organisationskultur unterliegen regelmäßiger Weiterentwicklung, welche durch die Mitarbeiter der DD-IT getragen und gelebt wird.

3.6 Sicherheitsmanagement

Zur Durchsetzung des Sicherheitsmanagements wurde ein strukturübergreifendes Informationssicherheits-Team (ISMT) gebildet. Dieses besteht aus dem Informationssicherheitsbeauftragten (ISB) und den Informationssicherheitsassistenten (ISA) aus allen Fachgruppen. Der ISB ist der Geschäftsführung direkt unterstellt.

Der ISB, das ISMT und die Geschäftsführung der DD-IT sind für die Erstellung von Maßnahmen und Prozessen zum sicheren Einrichten und Ausbauen eines dokumentierten Informationsmanagementsystems verantwortlich, auch wenn Aufgaben delegiert werden. ISB und ISMT erstellen Informationssicherheits-Richtlinien, -Prozesse und -Standards auf Grundlage von ISO 27001 und anderen sicherheitsrelevanten festgelegten Standards der ISO 27000 Reihe. Die Geschäftsführung der DD-IT trägt das Gesamtrisiko und entscheidet über die Umsetzung oder teilweise Umsetzung der erstellten Maßnahmen und Prozesse. Ausschließlich die Geschäftsführung der DD-IT entscheidet über das Maß des zu tragenden Restrisikos und trägt die Gesamtverantwortung für das Sicherheitskonzept.

Der ISB und das ISMT stellen die Entwicklung des ISMS und die damit verbundene kontinuierliche Weiterentwicklung sicher. Der ISB und das ISMT sind dafür verantwortlich, dass die aktuelle Sicherheitsleitlinie veröffentlicht wird.

Der ISB und das ISMT hat das Sicherheitsbewusstsein der Mitarbeiter in seinem Umfang und in seiner Qualität stetig zu verbessern.

Sicherheitsanalysen und die Einhaltung der Sicherheitsleitlinie liegen im Verantwortungsbereich der Geschäftsführung, des ISB und des ISMT.

3.7 Anforderungen an den Auftraggeber

Der Auftraggeber hat gemäß den Sicherheitsanforderungen die zu verarbeitenden Informationen, Daten und Datensammlungen so zu klassifizieren, dass die DD-IT das geforderte Sicherheitsniveau anwenden kann.

3.8 Durchsetzung

Die Durchsetzung der Sicherheitsleitlinie wird überprüft. Aus bewusstem Fehlverhalten ergeben sich unten beschriebene Konsequenzen.

3.9 Verstöße

Verstöße sind beabsichtigte oder grob fahrlässige Handlungen, welche:

- eine Kompromittierung der DD-IT darstellen,
- die Sicherheit der Mitarbeiter, Vertragspartner, Berater und die Werte der DD-IT kompromittieren,
- der DD-IT einen tatsächlichen oder potentiellen finanziellen Verlust einbringen, welche durch die Kompromittierung der Daten oder Informationen ursächlich ausgelöst wird.

Als Verstöße sind weiterhin zu betrachten:

- bewusster unbefugter Zugang zu Daten, Informationen oder besonders geschützten Bereichen,
- bewusster unbefugter Zugriff auf Daten, Informationen, Datensammlungen und andere Werte,
- unbefugte Preisgabe von Informationen, Daten oder Datensammlungen,
- die Änderungen von Daten, welche nicht rechtmäßig erworben wurden oder ungewollt in den eigenen Zugriffsbereich gelangt sind,
- die Nutzung von DD-IT eigenen Informationen zu illegalem Zweck.

3.10 Konsequenzen bei Fehlverhalten

Mögliche Konsequenzen, welche sich aus den Verstößen ergeben können, sind:

- Disziplinarische Maßnahmen,
- Entlassung,
- Straf- und/oder zivilrechtliche Verfahren,
- Einforderung von Schadenersatz für entstandenen finanziellen Schaden.

3.11 Sicherheitsdokumentation

- Die Sicherheitsdokumentation wird im Dokumentenmanagement des Informationsmanagementsystems (ISMS) hinterlegt und beinhaltet alle sicherheitsrelevanten Bereiche.
- Die Sicherheitsleitlinie, die Sicherheitsrichtlinien und die entsprechenden Standards sind einzuhalten.
- Als Richtlinie für den Sicherheitsstandard und zur Pflege des ISMS ist der Standard DIN ISO/IEC 27000 und folgende in der aktuell gültigen Fassung maßgeblich.
- Die Sicherheitsleitlinie gilt für die gesamte DD-IT.

4 Gültigkeit

Nach Bestätigung dieser Sicherheitsleitlinie durch die Geschäftsführung der DD-IT ist diese sofort gültig und für jeden Angestellten, jeden Vertragspartner, jeden Berater und jeden Zulieferer der bei oder für die DD-IT arbeitet, bindend.

5 Begriffe, Definitionen und Abkürzungen

Daten	dokumentierte Informationen
Datensammlungen	eine Zusammenstellung unabhängiger Daten, welche durch ihre Zusammenstellung ein Werk darstellt
ISB	Beauftragter der Geschäftsleitung für das Informationssicherheitsmanagement und Leiter des ISMT
ISA	Informationssicherheitsassistent und Mitglied des ISMT

ISMS	Informationssicherheitsmanagementsystem (engl. information security management system) gelebtes Konzept zur Behandlung von Sicherheitsvorfällen und zur Aufrechterhaltung des Sicherheitsniveaus
ISMT	Informationssicherheitsmanagementteam
ISO 27001	organisatorisch und technisch ausgerichtetes internationales Sicherheitskonzept; Internationale Norm
QMS	Qualitätsmanagementsystem