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

1 Zweck der Leitlinie

Die WOBCOM ist als Provider in entscheidendem Maße zur Erfüllung ihrer Geschäftsprozesse und um mit Kunden und Partnern zusammenarbeiten zu können, auf die Verfügbarkeit moderner Informations- und Kommunikationstechnik angewiesen. Darüber hinaus bestehen Verpflichtungen zur Gewährleistung der Informationssicherheit aufgrund gesetzlicher Bestimmungen und vertraglicher Verpflichtungen der WOBCOM gegenüber Projektpartnern, Mitarbeitern und Kunden.

Dem Schutz der Informations- und Kommunikationsinfrastruktur der WOBCOM vor Missbrauch, Manipulation, Störungen, dem Ausspähen vertraulicher Informationen usw. – kurz: der Informationssicherheit – kommt daher eine maßgebliche Bedeutung zu. Mangelnde Informationssicherheit kann zu Störungen bei der Aufgabenerfüllung führen, die die Leistungsfähigkeit der WOBCOM mindern und im Extremfall deren Geschäftsprozesse zum Erliegen bringen kann.

Vor diesem Hintergrund ist ein angemessenes Niveau der Informationssicherheit in den Geschäftsprozessen der WOBCOM GmbH als Informationssicherheitsmanagementsystem (ISMS) organisiert.

2 Geltungsbereich

Diese Leitlinie und alle damit verbundenen Regelungen gelten für die gesamte WOBCOM. Ebenso gilt diese für alle im Auftrag des Unternehmens arbeitenden Externen. Die Inhalte der Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen sind von allen Mitarbeitern der WOBCOM zu beachten und einzuhalten.

3 Ziele der Informationssicherheit

Alle Aktivitäten zur Aufrechterhaltung und Verbesserung der Informationssicherheit haben zum Ziel, die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und insbesondere unserer Kundendaten zu gewährleisten.

Die konkreten Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf der verarbeiteten Informationen stehen. Als Kernaktivitäten zur Aufrechterhaltung und Verbesserung der Informationssicherheit werden kontinuierlich Risiken für die Informationssicherheit identifiziert, bewertet und behandelt. An die Informationssicherheit werden verschiedene gesetzliche, behördliche und vertragliche Anforderungen gestellt, welche fortlaufend identifiziert und für die Informationssicherheit berücksichtigt werden.

4 Sicherheitsorganisation

Alle Verantwortlichkeiten der Informationssicherheit sind eindeutig zugewiesen.

Die Geschäftsführung übernimmt die Gesamtverantwortung für die Informationssicherheit bei der WOBCOM GmbH. Sie steht in vollem Umfang hinter den hier festgelegten Informationssicherheitszielen und den daraus abgeleiteten Konzepten, Richtlinien und Maßnahmen.

Zur Erreichung der Informationssicherheitsziele wurde ein Informationssicherheitsbeauftragter (ISB) von der Geschäftsführung benannt. Dieser berät die Geschäftsführung bei der Planung und Umsetzung der Informationssicherheit im Unternehmen. In seiner organisatorisch unabhängigen Funktion berichtet er regelmäßig und anlassbezogen direkt an die Geschäftsführung und wird bei seiner Arbeit von den Informationssicherheitskoordinatoren (ISK) der einzelnen Abteilungen unterstützt. Es wurde zudem ein Datenschutzbeauftragter (DSB) bestellt.

Die Geschäftsführung stellt dem ISB, den ISK und dem DSB die nötigen zeitlichen und finanziellen Ressourcen zur Verfügung, um sich weiterzubilden und die festgelegten Informationssicherheitsziele zu erreichen.

Der ISB wird frühzeitig in alle Projekte und Maßnahmen eingebunden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen.

5 Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme werden verantwortliche Personen (Asset-Verantwortliche) benannt, die den jeweiligen Schutzbedarf bestimmen und die notwendigen Zugriffsberechtigungen vergeben.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentation 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.

Alle Internetzugänge werden durch geeignete Firewall-Systeme 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 wieder aufgenommen 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 aufrechtzuerhalten 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 Geschäftsführung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Die aus den Sicherheitsmaßnahmen resultierenden Vorschriften und Regelungen in Form von Richtlinien sind allen Mitarbeitern der WOBCOM bekanntgegeben und verpflichtend einzuhalten.

6 Verbesserung der Informationssicherheit

Diese Leitlinie und das ISMS werden regelmäßig oder nach gravierenden Änderungen auf Aktualität und Wirksamkeit geprüft und angepasst. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, umsetzbar und in den Betriebsablauf integrierbar sind. Die Überprüfungen und die damit verbundenen Änderungen der Informationssicherheitsleitlinie werden von Resultaten der Managementbewertung beeinflusst. Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an den ISB weiterzugeben.

Der ISB informiert in geeigneter Form über die Aktualisierungen. Im Auftrag der WOBCOM handelnde Personen werden von dem zuständigen Ansprechpartner informiert.

Alle vorsätzlichen, grob fahrlässigen oder fahrlässigen Verstöße gegen Sicherheitsverfahren und -vorschriften werden von der WOBCOM anhand eines formalen Disziplinarprozesses verfolgt. Dieser basiert auf der Informationssicherheitspolitik und auf allen Leitlinien und Schutzmaßnahmen zu ihrer Unterstützung.

7 Mitwirkungspflichten

Die Geschäftsführung bekennt sich zu ihrer Aufgabe, die in dieser Leitlinie beschriebenen Zielsetzungen zur Informationssicherheit zu unterstützen und fordert alle Beschäftigten dazu auf, ebenfalls zur Aufrechterhaltung bzw. zur Verbesserung der Informationssicherheit beizutragen.