
1. Information Security Policy

1.1. Einleitung

Die Firma/Behörde ist von Informationen abhängig. Informationen entscheiden über unseren Erfolg und den unserer Kunden. Von größter Wichtigkeit ist neben der Genauigkeit und Verfügbarkeit in den meisten Fällen auch die Vertraulichkeit von Informationen. Jeder Mitarbeiter muß sich daher der Notwendigkeit der Informationssicherheit bewußt sein und entsprechend handeln. Diese Maßnahmen sind nicht nur gesetzlich vorgeschrieben, sondern auch Teil unserer Verpflichtungen gegenüber Aufsichtsbehörden und den Kunden. Jeder Mitarbeiter der Firma/Behörde muß sich daher an diese Policy und die daraus abgeleiteten Standards und Richtlinien halten.

Nach Maßgabe dieser Policy ist jede Geschäftseinheit der Firma/Behörde für die Sicherheit ihrer Informationen und einen angemessenen Schutz der Informationen entsprechend ihres Wertes und Risikos für das betreffende Geschäfts- oder technische Umfeld verantwortlich. Diese Anforderungen beinhalten, sind aber nicht allein darauf beschränkt, die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sowie die Rechenschaftspflicht des Einzelnen hinsichtlich der Nutzung von Informationen.

Diese Information Security Policy ist für jeden, der bei oder mit der Firma/Behörde (Angestellte, Vertragspartner, Berater oder Zulieferer) arbeitet, verpflichtend. Ihre Einhaltung wird überprüft.

Wir erwarten, daß jeder Mitarbeiter der Firma/Behörde diese Policy und die daraus abgeleiteten Standards und Richtlinien beachtet. Dazu zählt auch eine koordinierte Philosophie und globale IT-Infrastruktur der Firma/Behörde.

1.2. Sicherheitsbewußtsein

Die Informationssicherheit ist ein zunehmend wichtiger Faktor für Dienstleistungen auf einem wettbewerbsträchtigen Markt geworden. Daraus folgt, daß das Sicherheitsbewußtsein einer der entscheidenden Erfolgsfaktoren für die Firma/Behörde ist.

Sicherheitsbewußtsein ist durch folgendes Verhalten gekennzeichnet:


- Erkennen, daß effektive Sicherheit ein kritisches und wesentliches Element der Unternehmensphilosophie ist.
- Stets vorhandenes Sicherheitsbewußtsein bei allen täglich anfallenden Aktivitäten.
- Persönliche Verantwortlichkeit für proaktive Maßnahmen in bezug auf sämtliche Risiken für Mitarbeiter, Informationen, Vermögenswerte und die Fortführung der Geschäftstätigkeit im Notfall.

2. Grundsatzaussage

Die Informationen müssen so geschützt werden, daß

- die Vertraulichkeit in angemessener Weise gewahrt ist,
- die Integrität der Informationen sichergestellt ist,
- sie bei Bedarf verfügbar sind,
- die Beteiligung an einer Transaktion nicht geleugnet werden kann,
- gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen erfüllen kann.

Es wird verlangt, daß

-
- 
- für Informationen (Daten, unterstützende Systeme und Verfahren) namentlich Informationseigentümer ernannt werden und daß diese für die Festlegung des erforderlichen Kontrollumfangs verantwortlich sind,
 - der jeweils für die Informationen geltende Sicherheits- und Kontrollumfang am jeweiligen Geschäftsrisiko ausgerichtet ist,
 - die einzelnen Nutzer für die Nutzung der Informationen verantwortlich sind,
 - durch Erzeugung zusätzlicher Informationen und durch zusätzliche Verfahren die Nachvollziehbarkeit sämtlicher Transaktionen gewährleistet ist,
 - es eine unabhängige Überprüfung der Verwaltung und Nutzung von Informationen gibt.

2.1. Informationsklassifizierung und -kontrolle

Für alle Informationen muß es einen benannten Eigentümer geben. Insbesondere müssen für jedes der nachfolgenden Beispiele Informationseigentümer benannt sein:

- Informationen (Datenbanken, Magazine)
- Infrastruktur (abteilungs- oder firmenweite Infrastruktur, z. B. Netze)
- Geschäftsabwicklungsprozesse (end-to-end Arbeits- oder Transaktionsflüsse)

Der Informationseigentümer muß sicherstellen, daß

- geeignete Sicherheitsgrundsätze, Standards und entsprechende Richtlinien für die Informationsteile, die er direkt oder durch Ernennung zum Treuhänder besitzt, eingehalten werden,
- der für den Schutz spezifischer Informationen oder Verfahren insgesamt geltende Sicherheits- und Kontrollumfang der Sensitivität, dem Wert und der Bedeutung der Informationen (z. B. Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Verantwortlichkeit und Verbindlichkeit) der Maßgabe eines festgelegten Klassifizierungsverfahrens entspricht. Dieses Verfahren wird jeweils auf Bereichsebene festgelegt.

2.2. Systemzugangskontrolle

Die Firma/Behörde setzt logische und physische Zugangskontrollen ein, sowie abgesichertes Logging für sämtliche von ihr betriebenen Informationssysteme und Verfahren.

- Die Verantwortlichkeit und Rechenschaftspflicht für die Festlegung von Zugriffsrechten liegen bei den Informationseigentümern.
- Der Zugriff auf Informationen darf Nutzern nur für den definierten Geschäftsbedarf gewährt werden.

2.3. Sicherheit der Informationssysteme während des Lebenszyklus

- Eine Sicherheitsrisikoanalyse muß ein fester Bestandteil bei der Entwicklung, bei Einführungs- und
- Wartungsverfahren von Informationssystemen sein, und zwar ab Beginn des Lebenszyklus.
- Neue Hardware und/oder Software muß den geltenden Informationssicherheitsstandards:
 - Information Security Policy (ISP),
 - Generic Security Standards (GSS),
 - Product-based Operating Manuals (POM)

entsprechen.

3. Verantwortlichkeiten

3.1. Informationseigentümer

Der Informationseigentümer ist verantwortlich für:

- die Festlegung der geschäftlichen Relevanz seiner Informationen,
- die Festsetzung und Genehmigung des Sicherheits- und Kontrollumfangs, um in angemessener Weise die Sensitivität, den Wert und die Bedeutsamkeit seiner Informationen zu schützen und - sofern notwendig - die Vermeidung ungerechtfertigter Zurückweisungen, abhängig von der von ihm getroffenen Entscheidung bezüglich der Geschäftsrelevanz,
- die Sicherstellung, daß Verantwortlichkeiten explizit definiert und Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz seiner Informationen implementiert werden,
- die Sicherstellung, daß die Systeme, mit denen seine Informationen bearbeitet werden, regelmäßig hinsichtlich der Einhaltung der Information Security Policy und Standards geprüft werden.

Bei der Festlegung des für die betreffenden Informationen erforderlichen Sicherheits- und Kontrollumfangs sollte der Informationseigentümer die Art und Weise, wie Informationen erzeugt und verwaltet werden, sowie die geschäftliche Relevanz der Informationen entsprechend ihrer Bedeutung für das Geschäft, ihre Sensitivität, die erforderliche Vertrauenswürdigkeit, ihre Verfügbarkeit und Nicht-Ablehnbarkeit seitens ihrer Empfänger (Verbindlichkeit) berücksichtigen.

Der Informationseigentümer ist für den vergebenen Zugriff auf seine Informationen verantwortlich und muß ihre Zugänglichkeit sowie den Umfang und die Art der Autorisierung definieren, die im jeweiligen Zugriffsverfahren erforderlich ist. Bei diesen Entscheidungen ist folgendes zu berücksichtigen:

- die Notwendigkeit, die Informationen entsprechend ihrer geschäftlichen Relevanz zu schützen,
- inwieweit die für die jeweiligen Geschäftsanforderungen erforderlichen Informationen zugänglich sein müssen,
- die Aufbewahrungsvorschriften,
- die mit den Informationen verbundenen rechtlichen und aufsichtsrechtlichen Anforderungen.

Bei den Informationseigentümern muß es sich nicht notwendigerweise um eine Einzelperson handeln. Vielmehr kann diese Funktion durchaus auch von einem Lenkungsausschuß, einer Prüfkommision oder einer anderen offiziellen Einrichtung übernommen werden. Dabei sollte ebenfalls berücksichtigt werden, daß die Verwendung und das Sammeln von Informationen im Zuge der Bearbeitung oder Übertragung derselben in verschiedene Bereiche zu einem neuen Informationseigentümer führen kann.

3.2. Informationstreuhänder

Der Informationstreuhänder, der z. B. per Servicevertrag (Service Level Agreement oder Vollmacht) ernannt wurde, ist für die Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Rechenschaftspflicht, Verbindlichkeit der Informationen in dem vom Informationseigentümer festgelegten Umfang und nach Maßgabe der Bestimmungen dieser Policy verantwortlich. Der Informationstreuhänder ist verpflichtet, den Informationseigentümer über die Risiken zu informieren, die sich durch eine von dem Informationseigentümer getroffenen Kontroll- und Sicherheitsentscheidung ergeben können.

Wenn ein und derselbe Nutzer Informationen sowohl erzeugt als auch verwaltet, gilt er als Informationseigentümer und gleichzeitig als Informationstreuhänder.

3.3. Nutzer

Nutzer (Mitarbeiter, Vertragspartner, Berater) sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die Information Security Policy und die damit verbundenen Informationssicherheitsstandards sowie die Richtlinien des Unternehmens einzuhalten. Die einzelnen Nutzer sind für sämtliche Maßnahmen verantwortlich, die sie bei der Nutzung von Informationen und der damit verbundenen Systeme ergreifen.

Die Nutzer müssen verstehen, wann und warum Informationen, die von der Firma/Behörde zur Durchführung ihrer Geschäfte verwendet werden, durch angemessene Kontrollen geschützt werden sollten. Um diese Kontrollen durchführen zu können, sind sie verpflichtet, adäquate Unterstützung einzuholen. Die Firma/Behörde bietet Nutzern entsprechende Schulungen und Beratung über Informationssicherheit an.

Nutzer, die eine Verletzung der Information Security Policy und der damit verbundenen Informationssicherheitsstandards vermuten oder Kenntnis davon erlangt haben bzw. annehmen, daß Informationen nicht in geeigneter Weise geschützt sind, müssen dies unverzüglich ihrem Vorgesetzten und/oder einer lokal bzw. global zuständigen Sicherheitskontaktstelle melden.

3.4. Sicherheitsmanagement

Das Sicherheitsmanagement (Sicherheitsexperten-Team der Firma/Behörde) ist für eine sichere und solide Bearbeitung sämtlicher Transaktionen der Firma/Behörde nach Maßgabe der festgelegten Standards sowie für die Sicherstellung des Schutzes unserer Informationen und der unserer Kunden verantwortlich.

Das Sicherheitsmanagement stellt die Entwicklung der Information Security Policy und der damit verbundenen Standards, ihre ständige Fortschreibung und Veröffentlichung sicher. Es ist sowohl für die Einführung von Sicherheitsprogrammen entsprechend den geschäftlichen Bedürfnissen sowie für die Bereitstellung globaler Sicherheitsdienstleistungen zum Schutz der Firma/Behörde verantwortlich. Dazu zählen auch das Sicherheitsbewußtsein der Mitarbeiter, die Sicherheitsanalyse und - wenn erforderlich - die technische Überwachung. Das Sicherheitsmanagement versichert sich ständig über die Einhaltung dieser Policy.

Das Sicherheitsmanagement ist für die Eskalation nicht gewährleisteter Risikoübernahmen an die Geschäfts- bzw. Behördenleitung verantwortlich.

3.5. Unabhängige Prüfung

Die Verwaltung, Nutzung und Kontrolle von Informationen müssen von unabhängiger Seite überprüft werden. Bei dieser Prüfung muß die Stichhaltigkeit der Sicherheitsklassifizierung der Informationen begutachtet werden. In bezug auf diese beiden Faktoren ist die Angemessenheit der nachstehenden Eigenschaften wichtig:

- Zugriffsmöglichkeit zu den Informationen,
- Kontrollen im Zusammenhang mit den Informationen,
- Verwaltung der Informationen, einschließlich der Trennung von Rollen und unabhängige Genehmigung/Überprüfung von Transaktionen,
- Maßnahmen zur Wiederherstellung von Information und Verfahren.

4. Durchsetzung

4.1. Verstöße

Als Verstöße gelten beabsichtigte oder grob fahrlässige Handlungen, die

- eine Kompromittierung des Rufes der Firma/Behörde darstellen,
- die Sicherheit der Mitarbeiter, Vertragspartner, Berater und des Vermögens der Firma/Behörde kompromittieren,
- der Firma/Behörde tatsächlichen oder potentiellen finanziellen Verlust einbringen - durch die Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen,
- den unberechtigten Zugriff auf Informationen, deren Preisgabe und/oder Änderung beinhalten,
- die Nutzung von Unternehmens- bzw. Behördeninformationen für illegale Zwecke beinhalten.

4.2. Strafen

Die Nichteinhaltung oder bewußte Verletzung der Information Security Policy führt zu einer der nachfolgenden Aktionen, ist aber nicht auf diese beschränkt:


- Disziplinarmaßnahmen
- Entlassung
- straf- und/oder zivilrechtliche Verfahren.

5. Sicherheitsdokumentation

- Detaillierte Zielsetzungen und Anforderungen für Kontrollen zur Unterstützung dieser Information Security Policy (ISP) sind in den betreffenden Generic Security Standards (GSS) und in den Product-based Operating Manuals (POM) näher beschrieben.
- Sowohl die Policy als auch die betreffenden Standards müssen eingehalten werden.
- Die aktuelle Version des Grundschatzhandbuchs des Bundesamts für Sicherheit in der Informationstechnik (BSI) gilt solange standardmäßig als Generic Security Standards, bis spezifische, damit konforme globale Generic Security Standards, vorliegen.
- Weitere Informationen sind im Document of Standards (DoS) und/oder in den Product-based Operating Manuals beschrieben.
- Diese Policy gilt für den gesamte Firma/Behörde.

6. Anhang

Informationen	Daten, die gespeichert oder verwaltet werden auf Systemen oder Medien, wie z. B. auf Disketten, in der Infrastruktur oder im Rahmen von Geschäftsabläufen.
Sicherheit	Schutz von Informationsquellen vor unberechtigten Änderungen, Zerstörungen oder Preisgabe - unabhängig davon, ob sie absichtlich oder unabsichtlich erfolgten.
Vertraulichkeit	Vermeidung der Offenlegung von Informationen ohne Erlaubnis des Eigentümers.
Integrität	Vermeidung unberechtigter Änderungen, Erstellung oder Duplizierung von Informationen.



Verfügbarkeit	Vermeidung einer nicht annehmbaren Verzögerung bei der Durchführung eines genehmigten Zugriffs auf Informationen.
Authentizität	Grundsatz, daß der Empfänger zweifelsfrei sicher sein kann, daß eine Nachricht tatsächlich von dem angeblichen Verfasser geschaffen und nicht gefälscht wurde oder anderweitig durch Dritte verändert worden ist.
Rechenschaftspflicht	Grundsatz, daß Einzelpersonen für die Folgen ihrer Handlungen verantwortlich sind, die zu einer Verletzung der Sicherheit führen könnten oder bereits geführt haben.
Verbindlichkeit	Dieser Grundsatz besagt, daß später nachgewiesen werden kann, daß die an einer Transaktion Beteiligten die Transaktionen tatsächlich autorisiert haben und sie über keinerlei Mittel verfügen, ihre Beteiligung zu bestreiten.