

IT-Sicherheit Police der Swiss Remarketing

Inhaltsübersicht

- 1 Information
- 1.1 Einleitung
- 1.2 Sicherheitsbewusstsein
- 2 Grundsatzaussage
- 2.1 Informationsklassifizierung und -kontrolle
- 2.1.1 Backup-Sicherung
- 2.1.2 Backup-Wiederherstellung
- 2.2 Interne Netzwerksicherheit
- 2.3 Systemzugangskontrolle
- 2.4 Sicherheit der Informationssysteme während des Lebenszyklus
- 3 Verantwortlichkeiten
- 3.1 Applikations- & Datenowner
- 3.2 Externen IT-Leiter und externen IT-Provider
- 3.3 Nutzer
- 3.4 Unabhängige Prüfung
- 4 Durchsetzung
- 4.1 Verstösse
- 4.2 Strafen
- 5 Sicherheitsdokumentation
- 6 Glossar

1 Anwendungsbereich diese Datenschutzerklärung

1.1 Einleitung

Die Swiss Remarketing AG 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 Swiss Remarketing AG muss sich daher an diese Policy und die daraus abgeleiteten Standards und Richtlinien halten.

Nach Massgabe dieser Policy ist jede Geschäftseinheit der Swiss Remarketing AG 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 Swiss Remarketing AG (Angestellte, Vertragspartner, Berater oder Zulieferer) arbeitet, verpflichtend. Ihre Einhaltung wird überprüft.

Wir erwarten, dass jeder Mitarbeiter der Swiss Remarketing AG diese Policy und die daraus abgeleiteten Standards und Richtlinien beachtet.

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 Swiss Remarketing AG 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, Applikationen, 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 Klassifizierungs-Verfahrens entspricht. Dieses Verfahren wird jeweils auf Bereichsebene festgelegt.

2.1.1 Backup-Sicherung

Damit die Daten der Swiss Remarketing AG gesichert werden, ist ein Datensicherungssystem installiert, welche jede Nacht (Montag bis Freitag) eine Sicherungsjob ausführt und die kompletten Daten auf ein portables Tape sichert. Die Backup Tapes werden in einem feuersicheren Tresor aufbewahrt, welcher ständig abgeschlossen ist.

2.1.2 Backup-Wiederherstellung

Die Datenintegrität bzw, Funktionalität der gesicherten Daten, wird jeden Monat durch den IT-Verantwortlichen getestet. Mittels der Backup Software, wird monatlich eine Wiederherstellungs-Job ausgeführt.

2.2 Interne Netzwerksicherheit

Die interne Netzwerksicherheit der Swiss Remarketing AG ist wie folgt sichergestellt. Alle Firmen Räume der Swiss Remarketing sind immer verschlossen, auch während der Arbeitszeit. Der Netzwerkschrank und Serverschrank ist mittels Schloss gesichert.

2.3 Systemzugangskontrolle

Die Swiss Remarketing AG setzt physische Zugangskontrollen ein, sowie abgesichertes Login für sämtliche von ihr betriebenen Informationssysteme und Verfahren. Die Verantwortlichkeit und Rechenschaftspflicht für die Festlegung von Zugriffsrechten liegen bei den Applikations- & Datenowner. Der Zugriff auf Informationen darf Nutzern nur für den definierten Geschäftsbedarf gewährt werden.

2.4 Sicherheit der Informationssysteme während des Lebenszyklus

Eine Sicherheitsrisikoanalyse muss ein fester Bestandteil bei der Entwicklung, Einführung und Wartung von Informationssystemen sein. Neue Hardware und/oder Software muss den geltenden Informationssicherheitsstandards: Information Security Policy (ISP) unterstehen. Der IT-Leiter ist für die Umsetzung und Sicherstellung dieser Standards verantwortlich.

3 Verantwortlichkeiten

3.1 Applikations- & Datenowner

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 Externen IT-Leiter und externen IT-Provider

Der externe IT Leiter und die externen IT Provider, 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 Informationstrehänder ist verpflichtet, den Applikations- & Datenowner 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 Informationstrehänder.

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 Systemen ergreifen.

Die Nutzer müssen verstehen, wann und warum Informationen, die von der Swiss Remarketing AG 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 Swiss Remarketing AG 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 Unabhängige Prüfung

Die Verwaltung, Nutzung und Kontrolle von Informationen müssen von unabhängiger Seite (internem und externem Audit (SQS) gemäss Prozess "stetige Verbesserung" 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 Swiss Remarketing AG darstellen,
- die Sicherheit der Mitarbeiter, Vertragspartner, Berater und des Vermögens der Swiss Remarketing AG kompromittieren, der Swiss Remarketing AG tatsächlichen oder potentiellen finanziellen Verlust einbringen -durch die Kompromittierung der Sicherheit von Daten oder Geschäfts-Informationen, 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:

- Disziplinar-Massnahmen
- 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 Product-based Operating Manuals (POM) näher beschrieben.

Sowohl die Policy als auch die betreffenden Standards müssen eingehalten werden. Die aktuelle Version des Grundschutzhandbuchs des Bundesamts für Sicherheit in der Informationstechnik (BSI) gilt solange standardmäßig, bis spezifische, damit konforme globale Generic Security Standards, vorliegen. Weitere Informationen sind in POM beschrieben.

6 Glossar

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
Rechenschafts-Pflicht	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
Magazine	Magazine sind Ordner mit unternehmensspezifischen Daten

Version 3.0, Januar 2009