1. Informationssicherheitsrichtlinie

1.1. Einleitung

Die Landesfeuerwehrverbände / Behörden sind von Informationen abhängig. Von größter Wichtigkeit ist neben der Genauigkeit und Verfügbarkeit in den meisten Fällen auch die Vertraulichkeit von Informationen. Jeder FDISK-Nutzer 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 Feuerwehrmitgliedern. Jeder FDISK-Nutzer muss sich daher an diese Richtlinie und die daraus abgeleiteten Standards und Richtlinien halten.

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

Diese Informationssicherheitsrichtlinie ist für jeden, der in oder mit den Landesfeuerwehrverbände / Behörden (Mitarbeiter, Mitglieder, Vertragspartner, Berater oder Zulieferer) arbeitet, verpflichtend. Ihre Einhaltung wird überprüft.

Wir erwarten, dass FDISK-Nutzer diese Richtlinie und die daraus abgeleiteten Standards und Richtlinien beachten.

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 Landesfeuerwehrverbände / Behörden 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 Personen, 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 erfüllt werden können.

Es wird verlangt, dass

- für Informationen (Daten, unterstützende Systeme und Verfahren) namentlich Informationseigentümer benannt 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 Landesfeuerwehrverbände / Behörden setzen 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 Dienstgebrauch gewährt werden.

2.3. Sicherheit der Informationssysteme während des Lebenszyklus

• Eine Sicherheitsrisikoanalyse muss ein fester Bestandteil bei der Entwicklung, bei Einführung und
• Wartungsverfahren von Informationssystemen sein, und zwar ab Beginn des Lebenszyklus.
• Neue Hardware und/oder Software muss den geltenden Informationssicherheitsstandards:
Informationssicherheitsrichtlinie (ISR), Generic Security Standards (GSS), Product-based Operating Manuals (POM) entsprechen.

3. Verantwortlichkeiten

3.1. Informationseigentümer

Der Informationseigentümer ist verantwortlich für:
• die Festlegung der dienstlichen 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 Dienstrelevanz,
• 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 Informationssicherheitsrichtlinie 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 den Dienstgebrauch, 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 die Informationszugänglichkeit 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 Dienstanforderungen 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. 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 Richtlinie 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, Mitglieder, Vertragspartner, Berater) sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die Informationssicherheitsrichtlinie und die damit verbundenen Informationssicherheitsstandards sowie die Richtlinien der Landesfeuerwehrverbände / Behörden 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 Landesfeuerwehrverbänden / Behörden 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 Landesfeuerwehrverbände / Behörden bieten Nutzern entsprechende Schulungen und Beratung über Informationssicherheit an.

Nutzer, die eine Verletzung der Informationssicherheitsrichtlinie 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 (vorgesetzte melden.

3.4. Sicherheitsmanagement

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

Das Sicherheitsmanagement stellt die Entwicklung der Informationssicherheitsrichtlinie 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 Landesfeuerwehrverbände / Behörden 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 Richtlinie.

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 Landesfeuerwehrverbände / Behörden darstellen,
- die Sicherheit der Mitarbeiter, Mitglieder, Vertragspartner, Berater und des Vermögens der Landesfeuerwehrverbände / Behörden kompromittieren,

- den Landesfeuerwehrverbände / Behörden 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 Verbands- bzw. Behördeninformationen für illegale Zwecke beinhalten.

4.2. Strafen

Die Nichteinhaltung oder bewusste Verletzung der Informationssicherheitsrichtlinie 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 Informationssicherheitsrichtlinie (ISR) sind in den betreffenden Generic Security Standards (GSS) und in den Product-based Operating Manuals (POM) näher beschrieben.
- Sowohl die Richtlinie als auch die betreffenden Standards müssen eingehalten werden.
- Weitere Informationen sind in Generic Security Standards, Document of Standards (DoS) und/oder in den Product-based Operating Manuals beschrieben, die beim NÖ Landesfeuerwehrverband aufliegen.
- Diese Richtlinie gilt für die gesamten Landesfeuerwehrverbände / Behörden bei denen FDISK in Verwendung steht.

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.