

White Paper

## Policy & Compliance Management



NIIT IT-Sicherheit





## **Inhaltsverzeichnis**

1. Einleitung: Policies, Standards und Prozeduren .....	2
1.1 Policies (Richtlinien) .....	2
1.2 Standards .....	3
1.3 Prozeduren .....	4
2. Policy & Compliance Management.....	4
2.1 Ein stetiger Prozess, kein einmaliges Projekt .....	4
2.2 Der Prozess .....	5
2.3 Die zu adressierenden Bereiche .....	6
2.4 Policy Management .....	6
2.4.1 Erstellen oder Erweitern von Richtlinien.....	6
2.4.2 Educate .....	8
2.5 Compliance Management .....	9
2.5.1 Durchsetzen .....	9
2.5.2 Messen und Evaluieren.....	10
3. Fazit .....	10

## **Abbildungsverzeichnis**

Abbildung 1: Policies, Standards und Prozeduren .....	2
Abbildung 2: Prozess zur Durchsetzung von Policies .....	5
Abbildung 3: Anforderungsmatrix .....	6
Abbildung 4: Abdeckung der Anforderungsmatrix .....	11

# 1. Einleitung: Policies, Standards und Prozeduren

Der Begriff der Richtlinien bzw. Policies wird vielfach mit den unterschiedlichsten Bedeutungen belegt. Die folgende Definition zeigt, wie wir bei NIIT Technologies die Begriffe verwenden und verstehen.

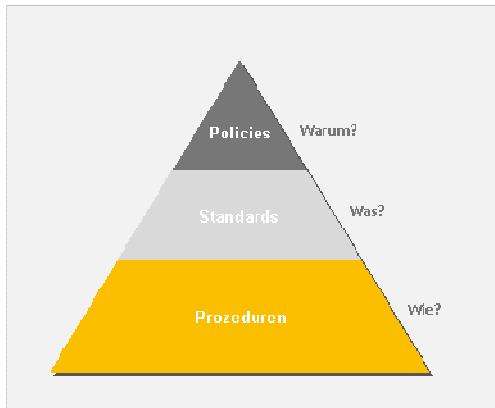


Abbildung 1: Policies, Standards und Prozeduren

## 1.1 Policies (Richtlinien)

Policies definieren den Grund der Informationssicherheit (Warum besteht Schutzbedarf?) und erfüllen folgende Anforderungen:

- Sie sind klare Management-Vorgaben und Anweisungen,
- stellen einen formalen Weg dar, um mitzuteilen „so wird es hier gemacht“,
- sind allgemeiner gehalten als Standards und Prozeduren und enthalten keine technischen Details,
- sind unabhängig von Produkten und
- stellen keine Empfehlungen dar, sondern sind verpflichtend.

Ein typisches Beispiel ist eine Kennwort-Richtlinie. Eine solche Policy könnte folgendermaßen formuliert sein:

Jeder Benutzer erhält jeweils ein individuelles Benutzerkonto für die benötigten IT-Systeme. Der Benutzer muss das Kennwort des Benutzerkontos vertraulich behandeln und muss alle seine Kennwörter nach den folgenden Kriterien vergeben:

- mindestens 8 Zeichen lang
- enthält Groß- und Kleinbuchstaben

- enthält mindestens eine Ziffer
- kein Wort aus einem Wörterbuch darf enthalten sein
- maximal 2 Zeichenpaare dürfen enthalten sein

Diese Beispielrichtlinie ist eindeutig und verbindlich und kann für die unterschiedlichsten Plattformen angewandt werden.

Als weiteres Beispiel hier eine Richtlinie zur sicheren Datenübertragung, die wie folgt formuliert sein könnte:

Da generell alle Netzwerke außerhalb des Unternehmens XYZ als unsicher anzusehen sind, müssen Daten und deren Übertragung aus diesen Netzen besonders geschützt werden. Um die Unternehmensdaten vor unautorisiertem Zugriff zu schützen, müssen beim elektronischen Datenaustausch mit dem Unternehmen von extern folgende Kriterien beachtet werden:

- Vor der Datenübertragung hat eine starke Authentifizierung stattzufinden.
- Die Datenübertragung hat nach aktuellen Standards verschlüsselt zu erfolgen (siehe Standards für elektronische Datenübertragung).

Das Endgerät hat zu jeder Zeit der Datenübertragung vor unautorisierten physischen und elektronischen Zugriffen von außen geschützt zu sein.

## 1.2 Standards

Während die Policies das „Warum?“ angeben, definieren die Standards das „Was?“.

Klare Unternehmensstandards werden vorgegeben und es werden Technologien, Verfahren, Produkte und Tools für die Umsetzung spezifiziert. Zur Verdeutlichung sei hier der Standard zur Policy für die sichere Datenübertragung aufgeführt:

Um eine sichere Datenübertragung von extern mit dem Unternehmen zu gewährleisten, sind mindestens folgende Technologien einzusetzen:

- Die Authentifizierung am Remotesystem sowie am Gateway hat über eine sog. Zwei-Faktoren-Authentifizierung stattzufinden. Dabei authentifiziert sich die Person durch den Besitz z.B. einer Smartcard und durch das Wissen der zugehörigen PIN. Hierzu muss die unternehmensweite Kobil SmartKey Lösung eingesetzt werden.
- Die verschlüsselte Übertragung der Daten hat mindestens mit einem starken, der Verschlüsselung zugeordneten Algorithmus stattzufinden. Dies ist nach heutigem Stand der Technik 3DES oder AES-256. Auf der Client-Seite wird hierfür standardmäßig unternehmensweit der Aventail VPN Client eingesetzt.

Ausnahmen bedürfen der Genehmigung durch den Chief Security Officer (CSO).

- Auf dem Endgerät muss zu jeder Zeit der Datenübertragung eine Firewall aktiv sein, die jegliche Zugriffe aus den externen Netzwerken blockt. Im Falle von Laptops wird unternehmensweit die F-Secure Anti-Virus Client Security verwendet.

### 1.3 Prozeduren

Prozeduren definieren, wie die Umsetzung oder Anwendung der Policies und Standards zu erfolgen hat. Im Fall der Datensicherung beispielsweise legt eine Policy fest, dass eine Sicherung der Unternehmensdaten zu erfolgen hat, beschreibt ein Standard, was gesichert werden muss, und definieren Prozeduren, wie Datensicherungen vorzunehmen sind.

## 2. Policy & Compliance Management

### 2.1 Ein stetiger Prozess, kein einmaliges Projekt

Leider wird Policy & Compliance Management häufig als ein gewaltiges Projekt angesehen, nach dessen erfolgreichen Abschluss sich alle wieder „gemütlich zurücklehnen und entspannen“, bis das nächste Projekt ansteht. Diese Vorgehensweise hat sich als schlechte, ineffiziente und sehr kostspielige Angelegenheit erwiesen.

#### Ein negatives Beispiel

Das Unternehmen XY, ein Automobilzulieferer, ist nach ISO 9001 zertifiziert. Dafür hat er im Rahmen einer großen Erstinvestition die erforderlichen Maßnahmen umgesetzt, um die notwendigen Prozesse und QM-Maßnahmen zu spezifizieren und zu dokumentieren. Doch anstatt die Prozesse umzusetzen, wird in der Produktion nach wie vor nach der alten Vorgehensweise gearbeitet, während das ISO-Handbuch in jeder Abteilung im Regal verstaubt. Immer kurz bevor ein erneutes Audit ins Haus steht, bricht eine zweiwöchige Panik aus, bei der alles auf Vordermann gebracht wird. Sobald die Auditoren wieder aus dem Haus sind, geht es im alten Stil weiter.

Was bedeutet dies für das Unternehmen und somit letztendlich für jeden Mitarbeiter?

- Das Unternehmen erfüllt vordergründig die Anforderung des Kunden, nach ISO 9001 zertifiziert zu sein und darf somit an den Kunden liefern.

- Das Unternehmen hat aufgrund der Diskrepanz zwischen Vorgaben und gelebter Praxis in Intervallen hohe Zusatzaufwendungen und damit Kosten.
- Das Unternehmen verschenkt ein Qualitätssteigerungs- und damit Kostenoptimierungspotential, da es mühselig erarbeitete Prozesse nicht umsetzt.
- Zusätzlich dazu führt diese Diskrepanz zu einer Frustration bei den Mitarbeitern.

Um diese Nachteile zu vermeiden, ist es von größter Bedeutung, das Thema Policy & Compliance Management als fortlaufenden Prozess zu verstehen und nicht als stets wiederkehrendes Projekt.

## 2.2 Der Prozess

Die Umsetzung des beschriebenen Prozesses verhindert nicht nur die negativen Auswirkungen einer projektbezogenen Vorgehensweise, sondern versetzt ein Unternehmen in die Lage, die folgenden Vorteile zu erzielen:

- Unternehmenswerte werden besser geschützt.
- Produktivitätsverluste durch Sicherheitsvorfälle werden minimiert.
- Die IT-Sicherheit wird vom reaktiven in den proaktiven Modus versetzt und wird damit zu einem Business-Enabler.
- Mitarbeiter erfahren durch die zusätzliche Übertragung von Verantwortung eine Aufwertung und sind dadurch stärker motiviert.
- Durch die aktive Einbindung der Mitarbeiter entsteht eine höhere Identifikation der Mitarbeiter mit dem Unternehmen.
- Ein höheres Momentum durch engagierte Mitarbeiter kann einen entscheidenden Wettbewerbsvorteil darstellen.



Abbildung 2: Prozess zur Durchsetzung von Policies

## 2.3 Die zu adressierenden Bereiche

Im Wesentlichen können die durch Policy & Compliance Management zu adressierenden Bereiche auf drei Kerngruppen aufgeteilt werden. Dies sind:

- Die Menschen und die akzeptable Internetnutzung
- Der Content und die Informationsklassifizierung
- Die Technologien und die technischen Sicherheitsstandards

Aus der Zuordnung der zu adressierenden Bereiche zu den einzelnen Prozessschritten ergibt sich zwangsläufig eine Anforderungsmatrix. Die ersten beiden Schritte können generell als Policy Management und die Schritte 3 und 4 als Compliance Management betrachtet werden.

	I Erstellen	II Educate	III Durchsetzen	IV Messen
Akzeptable Internet Nutzung				
Informationsklassifizierung				
Technische Sicherheitsstandards				

Abbildung 3: Anforderungsmatrix

## 2.4 Policy Management

### 2.4.1 Erstellen oder Erweitern von Richtlinien

Richtlinien zu etablieren bzw. etablierte Richtlinien zu erweitern, dient der Verminderung von Risiken. Ein Unternehmen, das keine Richtlinien etabliert, verhält sich wie ein Bauherr, der ein Haus ohne einen Bauplan und Berechnungen zur Statik baut. Dies würde niemandem einfallen. Doch gibt es immer noch viele Unternehmen, die ihre IT-Infrastruktur und ihr gesamtes Business ohne Richtlinien betreiben. Bei der Erstellung und Erweiterung von Richtlinien sollten folgende gängige Fehler vermieden werden:

- veraltete, unvollständige oder nur unzureichend zugängliche Richtlinien
- zu umfangreiche Richtlinien: Belastung des Einzelnen mit Informationen, die ihn nicht betreffen → Überflutung der Mitarbeiter mit Informationen

- zu komplizierte Richtlinien, formuliert in „Fach-Chinesisch“
- Widersprüche innerhalb der Richtlinie oder zwischen mehreren Richtlinien
- nicht als verbindliche Anordnung kommuniziert, kein Nachdruck zur Einhaltung
- nicht durchsetzungsfähig
- nicht überprüfbar

Die Etablierung von Richtlinien kann manuell erfolgen (so meist der Fall bei kleineren Unternehmen) oder durch Einsatz von entsprechenden Softwarelösungen, die den Lebenszyklus von Richtlinien unterstützen. Bei der Auswahl einer Softwarelösung sollten die folgenden Kernpunkte beachtet werden:

- Vorlagen mit „best practices“  
Eine Softwarelösung sollte nach der allgemein gültigen und anerkannten ISO 17799:2005 bzw. ISO 2700x aufgebaut sein und nach Möglichkeit eine Vielzahl an „best practices“-Policies mitliefern. Erfahrene Experten im Umgang mit Richtlinien können diese Vorlagen schnell und effizient auf das eigene Unternehmen anpassen.
- Elektronische Verteilung der Richtlinien  
Mit Hilfe der heutigen Webtechnologien können Richtlinien einfach über das Intra- und Extranet verteilt werden. Über entsprechende E-Mail-Erinnerungen bzw. -Informationen wird der betreffende Personenkreis über neue bzw. geänderte Richtlinien informiert. Die Benutzer können dann über ihre eindeutige Authentifizierung die für Sie relevanten Richtlinien in der aktuellen Fassung durchlesen.
- Implementierter Richtlinien Prozess  
Um Richtlinien so einfach und verständlich wie möglich zu halten, hat es sich als praktisch erwiesen, sie über einen klar definierten Prozess zu publizieren.

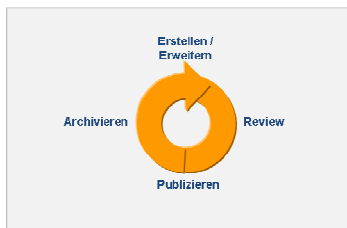


Abbildung 4: Prozess zur Durchsetzung von Policies

Dabei ist es vorteilhaft, wenn in dem Review-Gremium unterschiedliche Personengruppen (Geschäftsleitung, Risikomanagement u.a.) vertreten sind. Zum einen sollte dem Gremium neben dem Autor der Richtlinie(n) selbst noch mindestens eine weitere Person angehören, die fachliche Elemente überprüft und verifiziert. Zum anderen sollte mindestens eine zusätzliche Person involviert werden, die mehr mit der Anwenderseite vertraut ist und über keine spezifischen Fachkenntnisse verfügt, so wird schon im Vorfeld eine benutzerfreundliche Sprache sichergestellt und „Fach-Chinesisch“ vermieden.

## 2.4.2 Educate

Um die erstellten Policies erfolgreich umzusetzen und nicht wie im Automobilzulieferer-Beispiel im Schrank verstauben zu lassen, sind folgende Punkte von elementarer Bedeutung:

- Rollenbasierte Verteilung der Policies verhindert Informationsüberflutung.
- Policies sollten elektronisch zugänglich sein.
- Benutzer sollten verpflichtet sein, die Policies elektronisch als gelesen, akzeptiert und verstanden abzuzeichnen.
- Das Verständnis der Benutzer sollte überprüft und ein Awareness-Programm aufgesetzt werden, das den Benutzern die Wichtigkeit der Policies vermittelt.

Awareness trägt wesentlich zum Erfolg des Prozesses bei, darum wird dieser Themenbereich hier etwas ausführlicher behandelt.

Eine wichtige Komponente des Awareness Programms können Quizze sein, die mit gezielten Multiple-Choice Fragen zu den Policies das Verständnis der Mitarbeiter abprüfen. Bei der Online-Auswertung der Antworten können dann sowohl Benutzer als auch Administratoren wertvolle Hintergründe erkennen, um die richtigen Antworten zu verstehen und damit das Verständnis für die Policy zu vertiefen. Die größte Nachhaltigkeit wird bei einem Benutzer stets dann erreicht, wenn er die Sinnhaftigkeit einer Policy nachvollziehen kann.

Ein paar gute Gründe für ein Awareness Programm:

- Nutzen Sie die Energie ihrer Mitarbeiter, um das Unternehmen zu schützen.
- Überwinden Sie natürliche Impulse und trainierte Höflichkeit.
- Geben Sie klare Anweisungen an die Hand.
- Übertragen Sie Ihren Mitarbeitern Verantwortung und zeigen Sie so Ihre Wertschätzung.

- Die Einhaltung von Informationssicherheit ist für Ihre Mitarbeiter keine natürliche Sache und erfordert Vermittlung und Erklärung.
- Verwandeln Sie das schwächste Glied der Verteidigungskette, den Benutzer, in die erste Verteidigungslinie.

Entscheidend für den Erfolg von Awareness Programmen ist oftmals nicht der finanzielle oder zeitliche Aufwand, sondern vielmehr die Kreativität und Originalität, mit der die Aktionen durchgeführt werden. Also lassen Sie Ihrer Fantasie freien Lauf!

## 2.5 Compliance Management

### 2.5.1 Durchsetzen

Unternehmen müssen die Richtlinien auf der Ebene der Menschen und der Technologien durchsetzen. Eine nur technologische Umsetzung von Policies und Standards verfehlt bei weitem den Wirkungsgrad gegenüber einer Umsetzung für Menschen und Technologien.

Für die zu adressierenden Bereiche des Policy & Compliance Managements ergeben sich folgende zu implementierenden Lösungen:

- Akzeptable Internet-Nutzung  
Die Einhaltung der Policy zur akzeptablen Internetnutzung sollte über entsprechende Content Security Lösungen durchgesetzt werden:
  - Netzwerküberwachung (Firewalling, Intrusion Detection)
  - Anti-Virus
  - E-Mail und IM Content Kontrolle und Verschlüsselung
  - Kontrolle des Web Traffic (HTTP, HTTPS, FTP)

Detailliertere Ausführungen hierzu finden Sie in unserem White Paper „Richtlinienbasierte Content Security“.

- Informationsklassifizierung  
Die Durchsetzung der Richtlinie für die Informationsklassifizierung und vor allem die Überwachung der Einhaltung der Vorgaben sollte auf mehreren Ebenen erfolgen. Zum einen muss die Einordnung der Information in die entsprechende Klassifizierungsstufe durch entsprechende Prozesse abgedeckt werden. Zum anderen sollte der Zugriff bzw. das Versenden und der Erhalt von Informationen gemäß der Richtlinie kontrolliert werden.  
Für die Kontrolle des Zugriffs auf Daten auf den Servern kann ein hostbasiertes IDS-System eingesetzt werden, das Zugriffe auf geschützte

Verzeichnisse protokolliert und Zugriffsverletzungen umgehend an ein zentrales Security Information and Event Management-System meldet.

Die Einhaltung der Informationsklassifizierung beim Versand und Empfang von Daten kann über entsprechende Gateway Lösungen für E-Mail, Web und Instant Messaging implementiert werden. Details zu diesem Thema finden Sie in unserem White Paper „Richtlinienbasierte Content Security“.

- Technische Sicherheitsstandards

Die Durchsetzung von technischen Sicherheitsstandards kann in größeren Netzwerken mit mehreren Servern nur durch die Implementierung von Softwarelösungen erreicht werden, die einen hohen Grad an Automatisierung gewährleisten.

Dabei werden vorwiegend sicherheitsrelevante, technische Einstellungen auf den vorhandenen Betriebssystemen überprüft, wie Windows, Unix, Linux, Novell, OS/400 und OS/390, sowie auf geschäftskritischen Anwendungen, wie Datenbanken und Webservern.

### 2.5.2 Messen und Evaluieren

Die Messung bzw. Evaluierung der Umsetzung von Sicherheitsrichtlinien ist für die Einhaltung der Sicherheitsrichtlinien und -standards von grundlegender Bedeutung. Natürlich sollte die Evaluierung der Richtlinienkonsistenz wiederum für Menschen und Technologien durchgeführt werden. So ist es zwingend notwendig, dass alle Benutzer die Sicherheitsrichtlinien und -standards lesen und sich schriftlich verpflichten diese einzuhalten.

Es sollte zudem ein System für Security Information and Event Management etabliert sein, das sicherheitsrelevante Vorfälle aufzeigt und verfolgt.

Die Technologien sollten in regelmäßigen, am besten in automatisierten Intervallen und Prozessen anhand der Sicherheitsstandards geprüft, und Abweichungen über den Schwachstellen-Management-Prozess behoben oder geschäftsbedingte Abweichungen von den Standards dokumentiert werden.

## 3. Fazit

Das Policy & Compliance Management ist ein komplexes Thema, das prozessgestützt implementiert und gelebt werden muss, mit Boardmitteln von Betriebssystemen und

Standardsoftware nicht effizient gemeistert werden kann und eine integrierte Lösung benötigt, in der die einzelnen Software-Lösungen nahtlos ineinander greifen. Unsere Partnerfirmen bieten hervorragende Lösungen für intelligentes Policy & Compliance Management. Die Abdeckung der Anforderungsmatrix sieht dabei wie folgt aus:

	I Etablieren	II Educate	III Durchsetzen	IV Messen
Akzeptable Internetnutzung	<input checked="" type="checkbox"/> VigilEnt Policy Center	<input checked="" type="checkbox"/> VigilEnt Policy Center	<input checked="" type="checkbox"/> Marshal und F-Secure Produkte  <input checked="" type="checkbox"/> NetIQ Secure Configuration Manager	<input checked="" type="checkbox"/> Marshal und F-Secure Produkte  <input checked="" type="checkbox"/> NetIQ Secure Configuration Manager
Informationsklassifizierung	<input checked="" type="checkbox"/> VigilEnt Policy Center	<input checked="" type="checkbox"/> VigilEnt Policy Center	<input checked="" type="checkbox"/> Marshal Produkte	<input checked="" type="checkbox"/> Marshal Produkte
Technische Sicherheitsstandards	<input checked="" type="checkbox"/> VigilEnt Policy Center	<input checked="" type="checkbox"/> VigilEnt Policy Center	<input checked="" type="checkbox"/> NetIQ Secure Configuration Manager	<input checked="" type="checkbox"/> NetIQ Secure Configuration Manager

Abbildung 4: Abdeckung der Anforderungsmatrix

---

## NIIT Technologies

Die NIIT Technologies GmbH hat sich auf Services rund um Anwendungsentwicklung und -Management, IT-Security, IT-Infrastruktur und Managed Services spezialisiert und begleitet Kunden individuell von der strategischen Ausrichtung bis hin zur operativen Umsetzung. NIIT Technologies gehört zu den führenden Outsourcing-Anbietern weltweit. Neben unseren Kunden bestätigen das auch die Black-Book Studie 2009 und das Ranking der IAOP 2009.

## Ihr Ansprechpartner



**Michael Eisenmann**  
IT-Security Consultant

NIIT Technologies GmbH  
Zettachring 6 | 70567 Stuttgart

Tel: +49 7 11 71917 – 0  
michael.eisenmann@niit-tech.de  
www.niit-tech.de

**NIIT Technologies GmbH**

Deutschland  
Zettachring 6  
70567 Stuttgart  
Tel: +49 7 11 71917 - 0  
Fax: +49 7 11 71917 - 150

Delitzscher Straße 9  
40789 Monheim  
Tel: +49 21 73 16 75 - 0  
Fax: +49 21 73 16 75 - 150

[info@niit-tech.de](mailto:info@niit-tech.de)  
[www.niit-tech.de](http://www.niit-tech.de)

**NIIT Technologies GmbH**

Österreich  
Kandlgasse 18/4/9  
1070 Wien  
Tel: +43 1 729 62 62  
Fax: +43 1 729 62 62-90

[info@niit-tech.at](mailto:info@niit-tech.at)  
[www.niit-tech.at](http://www.niit-tech.at)

**NIIT Technologies AG**

Schweiz  
Tribtschenstraße 9  
6005 Luzern  
Tel: +41 41 360 48 77  
Fax: +41 41 360 21 64

[info@niit-tech.ch](mailto:info@niit-tech.ch)  
[www.niit-tech.ch](http://www.niit-tech.ch)

