Branchenempfehlung Strommarkt Schweiz

Richtlinien für die Datensicherheit von intelligenten Messsystemen, Anhang 2

Betriebliche Anforderungen an intelligente Messsystem für die Datensicherheit

RL-DSP – CH, Anhang 2, Ausgabe 2018

swissmig

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Telefon +41 62 825 25 25, Fax +41 62 825 25 26, info@strom.ch, www.strom.ch

VSE AES

Impressum und Kontakt

Herausgeber
Verband Schweizerischer Elektrizitätsunternehmen VSE
Hintere Bahnhofstrasse 10, Postfach
CH-5001 Aarau
Telefon +41 62 825 25 25
Fax +41 62 825 25 26
info@strom.ch
www.strom.ch

Druckschrift Nr. 1045 d, Ausgabe 2018

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Gültigkeitsbereich

(1) Im Dokument „Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz“, BfE 11/2014, [2], auch oft als „Mindestanforderungen“ bezeichnet, ist die Architektur eines intelligenten Messsystems (iMS) definiert worden (Abbildung 1).

(2) Diese Definition ist in der Stromversorgungsverordnung (StromVV) Änderung vom 1. November 2017, [6], Artikel 8a, Absatz 1, formal ausformuliert:

> Für das Messwesen und die Informationsprozesse sind bei den Endverbrauchern und den Erzeugern intelligente Messsysteme einzusetzen. Diese bestehen aus folgenden Elementen:
>
> a. einem elektronischen Elektrizitätszähler beim Endverbraucher oder Erzeuger, der:
>
> 1. Wirkenergie und Blindenergie erfasst,
> 2. Lastgänge mit einer Periode von fünfzehn Minuten ermittelt und mindestens sechzig Tage speichert,
> 3. über Schnittstellen verfügt, wovon eine zur bidirektionalen Kommunikation mit einem Datenbearbeitungssystem reserviert ist und eine andere für den Endverbraucher oder den Erzeuger, die ihm mindestens ermöglicht, Messwerte im Moment ihrer Erfassung sowie die Lastgänge nach Ziffer 2 abzurufen, und
> 4. Unterbrüche der Stromversorgung erfasst und protokolliert;
>
> b. einem digitalen Kommunikationssystem, das die automatisierte Datenübermittlung zwischen dem Elektrizitätszähler und dem Datenbearbeitungssystem gewährleistet; und
>
> c. einem Datenbearbeitungssystem, mit dem die Daten abgerufen werden.

(3) Die Definitionen werden durch das intelligente Messgerät (Art. 8a, Absatz 1, Buchstabe a), ein Kommunikationssystem (Datenkonzentrator bzw. Gateway) (Art. 8a, Absatz 1, Buchstabe b) und ein Head End System (Art. 8a, Absatz 1, Buchstabe c) abgedeckt.

(4) Im Weiteren müssen für das Gesamtsystem datensicherheits- und datenschutzrelevante Komponenten zusätzlich berücksichtigt werden:

- Meter Data Management System
- Visualisierungssysteme
  - lokal am iMG (Art. 8a, Absatz 1, Buchstabe a, 3.) als Schnittstelle
  - über eine Web-Plattform
- Ablese- und Konfigurationsgerät
- Server- Netzwerk- und Sicherheits-Infrastruktur
- Managementsystem für Kryptografische Schlüssel als zentraler Sicherheitsanker
- Übergeordnete Systeme zur Datenbearbeitung

(5) Für Datenmanager ergibt sich gemäss Artikel 8b keine formale Datensicherheitsprüfung. Die hier vorliegenden Anforderungen fordern dennoch interne und externe Prüfung in definierten Bereichen.

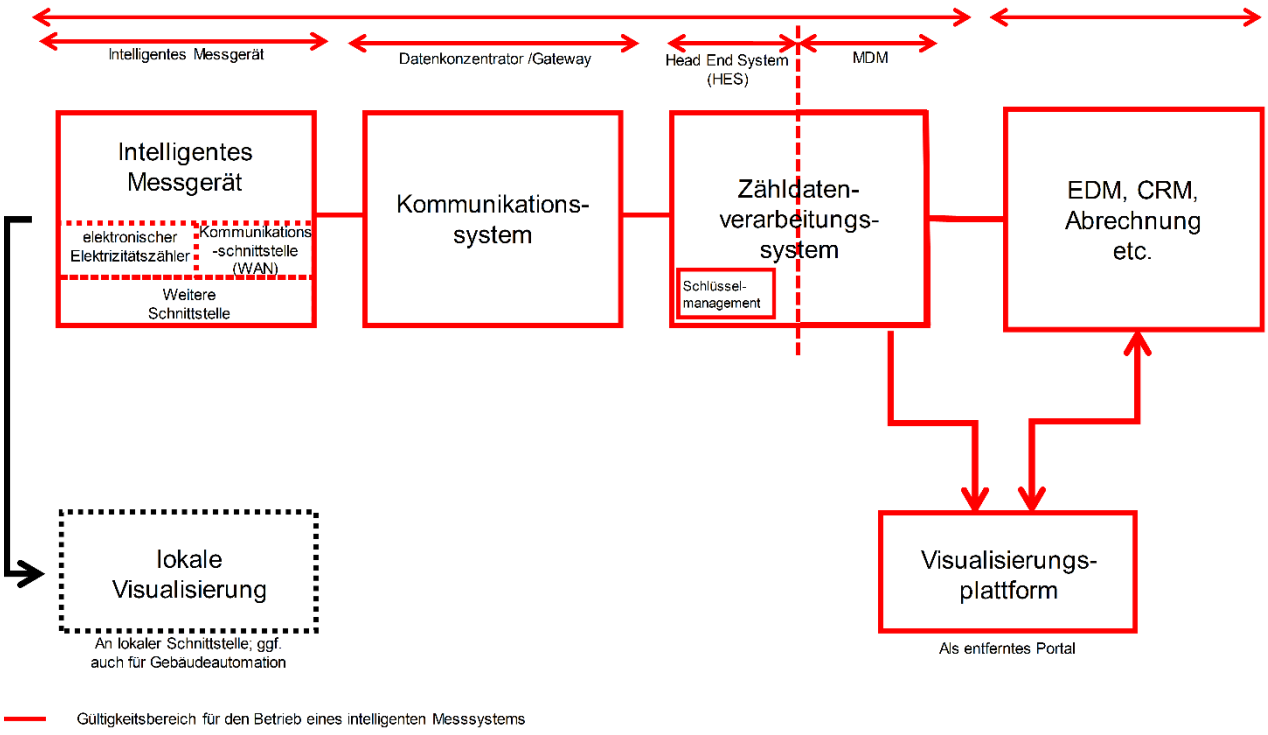

Abbildung 1 Gültigkeitsbereich intelligentes Messsystem für den Datenmanager

(6) Für das in der Abbildung 1 dargestellte Gesamtsystem ist zu gewährleisten, dass der Datenmanager (die Betreiber der Smart Metering Systems) nicht nur aus Sicht der Datensicherheit vertrauenswürdige Hauptkomponenten zurückgreifen können, sondern gleichzeitig die Qualifikation besitzen, entsprechende Systeme in ihren IT-Landschaften auf vertrauenswürdige Weise zu implementieren, auszurollen und zu betreiben.

(7) In diesem Gesamtsystem werden explizit keine unternehmensweite Sicherheitsanforderungen, u.a. strategische, taktische, organisatorische oder auch personelle Sicherheitsaspekte betrachtet.

1.1 Prämissen

Verwendung der Dokumente

(1) Das vorliegende Dokument enthält Anforderungen an die Implementation, den Rollout sowie den Betrieb des intelligenten Messsystems (iMS).

(2) Der Anhang 1 enthält Anforderungen an die Hauptkomponenten eines iMS und damit mittelbar an die Hersteller derselben. Die Anforderungen werden in Architektur und Funktionalität der Hauptkomponenten umgesetzt, und Korrektheit und Wirksamkeit werden durch eine Konformitätsprüfung nachgewiesen. Die erfolgreiche Konformitätsprüfung der Hauptkomponenten intelligentes Messgerät, Kommunikationssystem und HES sagen aus, dass der Datenmanager das intelligente Messsysteme sicher betreiben kann.

Zusätzliche Aspekte

(1) Das Schlüsselmanagement als Subsystem des Zähldatenverarbeitungssystems (ZDVS) wird ebenfalls auf die Erfüllung der im Anhang 1 formulierten Anforderungen geprüft. Die betrieblichen Prozesse zum Schlüsselmanagement liegen aber auch hier in der Verantwortung des Datenmanagers.

(2) Die Erfüllung der Anforderungen an Datensicherheit und Datenschutz muss vom Betreiber der entfernten Visualisierung gewährleistet werden. Falls die entfernte Visualisierung bi-direktionalen Datenverkehr mit einem der „übergeordneten Systeme“ aufweist, muss die Erfüllung der Anforderungen von den Betreibern beider Systeme gewährleistet werden.

(3) Die Datensicherheit muss vom Herausgeber einer lokalen Visualisierung gewährleistet werden.

2. Anforderungen adressieren die relevanten Schutzobjekte und Bedrohungen

(1) Die Hauptkomponenten des intelligenten Messsystems sind zertifiziert. Die Anforderungen an die Zertifizierung leiten sich an der Schutzbedarfsanalyse (SBA) ab. Damit eine umfassende Sicherheit des intelligenten Messsystems gleichermassen auch in der Inbetriebnahme, im Betrieb und nach Ausserbetriebnahme der Hauptkomponenten gewährleitet ist, werden nachfolgenden Anforderungen an den Datenmanager definiert. Die Anforderungen gelten zudem in Sinne der Datensicherheit und des Datenschutzes von intelligenten Messsystemen auch für die Umsysteme, welche der Datenmanager implementiert und betreibt.

(2) Die Anforderungen an das intelligente Messsystem adressieren die aufgezeigten Risiken der SBA und wurden auf Basis des international anerkannten Security Frameworks ISO/IEC 27002/27019 erstellt. Es wurden diejenigen Themen, Controls und Kriterien ausgewählt, welche eine risikominimierende Wirkung in der Implementierung, im Rollout und im Betrieb eines intelligenten Messsystems bewirken. Die folgenden Themen sind Teil der Anforderungen an den Datenmanager:

- Anforderungen an die Handhabung von Assets
- Anforderungen an die Zugriffskontrolle
- Anforderungen an das Schlüsselmanagement
- Anforderungen an die physische und gerätebezogene Sicherheit
- Anforderungen an den sicheren ICT Betrieb
- Anforderungen an die Kommunikationssicherheit
- Anforderungen an die Systemlieferantenbeziehungen
- Anforderungen an das Management von Informationssicherheitsvorfällen
- Compliance Anforderungen

(3) Explizit nicht Teil der folgenden Anforderungen sind unternehmensweite Governance-Themen, die zwar ebenfalls risikominimierend wirken, jedoch vom Datenmanager auch für andere sicherheitsrelevante Bereiche umgesetzt werden z.B. für den Umgang mit Mitarbeiterdaten oder für den Grundschutz von OT Umgebungen. Die folgenden Themen sind deshalb nicht Teil der nachfolgenden Anforderungen an den Datenmanager:

- Anforderungen an die Informationssicherheitspolitik
- Anforderungen an die Organisation der Informationssicherheit
- Anforderungen an die Personalsicherheit
- Anforderungen an das Business Continuity Management

(4) Ebenfalls nicht thematisiert ist die sichere Entwicklung von Systemen, da die Hauptkomponenten mit einem Zertifikat ausgeliefert werden, welche diesen Aspekt sicherstellen sollten. Bei allfälligen Eigenentwicklungen von Umsystemen muss der Datenmanager ergänzende Anforderungen an die sichere Entwicklung definieren.

(5) Nachfolgend sind generische Rollen des Datenmanagers definiert. Die Rollen sind als mögliche Umsetzungsverantwortliche zu verstehen können in der Praxis aber auch anders heissen oder auch von einem Lieferanten gestellt werden:

- Assetverantwortlichen: Die organisatorische Rolle ist wie der Name bereits sagt, verantwortlich für ein Asset- oder einer Gruppe von Assets. Assets auch Vermögenswerte genannt können nebst technischen Komponenten auch Informationen oder Prozesse sein. Typische Assetverantwortliche in der Informationssicherheit sind der Datenowner oder der Applikationsverantwortliche
- Benutzer: Es wird prinzipiell zwischen der Rollen der Anwender seitens Datenmanager (Benutzer), der Kunden (Endbenutzer) und Administratoren unterschieden.
- Breaker-Manager: Der Breaker Manager ist eine technische Rolle. Diese Rolle hat das Rechte Breaker Befehle zu steuern. Im iMS ist dies eine hoch privilegierte Funktion.
- Relais-Manager: Der Relais Manager ist eine technische Rolle. Diese Rolle hat das Rechte Relais Befehle zu regeln und steuern. Im iMS ist dies eine hoch privilegierte Funktion.

(6) Das detaillierte Security Rational, sprich die detaillierte Begründung, welche Themen, Controls und Kriterien für die nachfolgenden Anforderungen ausgewählt wurden und welche Risiken aus der SBA damit adressiert werden, kann auf Anfrage beim VSE eingesehen werden.

3. Anforderungen an die Handhabung von Assets

3.1 Inventar und Verantwortlichkeit für Assets

Ziel: Identifizierung von Assets (Informationen, Hard- & Software-Komponenten) innerhalb des intelligenten Messsystems und Definition der Aufgaben und Verantwortlichkeiten.

Inventarliste von Assets

Control 3.1.1 **Smart Meter**

(1) Sämtliche intelligenten Messgeräte müssen durch den Datenmanager identifiziert und in einem Inventar festgehalten sein. Das genannte Inventar muss stets aktuell gehalten werden.

a) Jeder Smart Meter muss eindeutig identifizierbar sein.
b) Mindestens die Installationslokation, die Firmware Version sowie die Seriennummer müssen im Inventar aufgeführt werden.

Control 3.1.2 **Kommunikationssystem**

(1) Sämtliche Komponenten von Kommunikationssystemen müssen durch den Datenmanager identifiziert und in einem Inventar festgehalten sein. Das genannte Inventar muss stets aktuell gehalten werden. Zu inventarisieren sind die Hardware und Software der Kommunikationskomponenten, die in der Betriebsverantwortung des Datenmanagers liegen, wie zum Beispiel *PLC Modems oder SIM Kommunikationsmodule* aber auch Services von Providern.

a) Jedes Element muss eindeutig identifizierbar sein.
b) Mindestens die Installationslokation, die Software Version sowie die Seriennummer müssen im Inventar aufgeführt werden.

Control 3.1.3 **Zähldatenverarbeitungssystem**

(1) Sämtliche Zählerdaten verarbeitende Systeme müssen durch den Datenmanager identifiziert und in einem Inventar festgehalten sein. Das genannte Inventar muss stets aktuell gehalten werden. Zu inventarisieren sind ebenfalls die darunterliegenden Server-, Sicherheits- und Netzwerkinfrastrukturen.

a) Jede Komponente (Hardware und Software) muss eindeutig identifizierbar sein.
b) Mindestens die Software sowie Betriebssystem Version(en) müssen im Inventar aufgeführt werden.

Control 3.1.4 **Ablese- und Konfigurationsgerät**

(1) Sämtliche Ablese- und Konfigurationsgeräte müssen durch den Datenmanager identifiziert und in einem Inventar festgehalten sein. Das genannte Inventar muss stets aktuell gehalten werden.

a) Jedes Ablese- und Konfigurationsgerät muss eindeutig identifizierbar sein.
b) Mindestens die Software und Betriebssystem Version, der Besitzer (Mitarbeitende) sowie die Seriennummer müssen im Inventar aufgeführt werden.

Verantwortlichkeiten von Assets

Control 3.1.5 **Smart Meter**

(1) Jede Komponente innerhalb des Inventars von intelligenten Messgeräten muss im Betrieb über einen Assetverantwortlichen verfügen.

a) Der Assetverantwortliche muss sicherstellen, dass seine intelligenten Messgeräte bzw. die Daten korrekt klassifiziert und geschützt sind.
b) Der Assetverantwortliche muss das Inventar jährlich einem stichprobenbasierten Review unterziehen.
c) Der Assetverantwortliche ist dafür verantwortlich, dass seine intelligenten Messgeräte nach der Stilllegung korrekt vernichtet werden.

Control 3.1.6 **Kommunikationssystem**

(1) Jede Komponente innerhalb des Inventars des Kommunikationssystems muss im Betrieb über einen Assetverantwortlichen verfügen.

a) Der Assetverantwortliche muss sicherstellen, dass seine Assets korrekt klassifiziert und geschützt sind.
b) Der Assetverantwortliche muss das Inventar jährlich einem stichprobenbasierten Review unterziehen.
c) Der Assetverantwortliche ist dafür verantwortlich, dass seine Assets nach der Stilllegung korrekt vernichtet werden.

Control 3.1.7 **Zähldatenverarbeitungssystem**

(1) Jede Komponente innerhalb des Inventars von Zähldatenverarbeitungssystem muss im Betrieb über einen Assetverantwortlichen verfügen.

a) Der Assetverantwortliche muss sicherstellen, dass seine Assets korrekt klassifiziert und geschützt sind.
b) Der Assetverantwortliche muss das Inventar jährlich einem stichprobenbasierten Review unterziehen.
c) Der Assetverantwortliche ist dafür verantwortlich, dass seine Assets nach der Stilllegung korrekt vernichtet werden.

Control 3.1.8 **Ablese- und Konfigurationsgerät**

(1) Das Inventar von Ablese- und Konfigurationsgeräten muss im Betrieb über einen Assetverantwortlichen verfügen.

a) Der Assetverantwortliche muss sicherstellen, dass seine Assets korrekt klassifiziert und geschützt sind.
b) Der Assetverantwortliche muss das Inventar jährlich einem stichprobenbasierten Review unterziehen.
c) Der Assetverantwortliche ist dafür verantwortlich, dass seine Assets nach der Stilllegung korrekt vernichtet werden.

Rückgabe von Assets

Control 3.1.9 **Kommunikationssystem**

(1) Tools zur Installation und dem Betrieb von Kommunikationssystemen sowie dafür verwendete Informationen müssen nach Beendigung von Arbeitsverhältnissen und Ablauf von Verträgen retourniert werden.

a) 'Die Rückgabe muss nachweislich erfolgen und ist durch den Assetverantwortlichen beim Datenmanager zu kontrollieren.
b) Eine Rückgabevereinbarung ist durch den Besitzer der Informationen und Tools zu unterzeichnen.

Control 3.1.10 **Ablese- und Konfigurationsgerät**

(1) Ablese- und Konfigurationsgeräte zur Installation und Parametrierung des intelligenten Messgeräts, sowie dafür verwendete Informationen müssen nach Beendigung von Arbeitsverhältnissen und Ablauf von Verträgen retourniert werden.

a) Die Rückgabe muss nachweislich erfolgen und ist durch den Assetverantwortlichen beim Datenmanager zu kontrollieren.
b) Eine Rückgabevereinbarung ist durch den Besitzer des Geräts zu unterzeichnen.

3.2 Klassifikation von Informationen

Ziel: Sicherstellen, dass Informationen entsprechend ihrem Schutzbedarf betreffend geschützt werden.

Klassifikation von Informationen

Control 3.2.1 **Übergreifende Schutzanforderung**

(1) Datenmanager als Betriebsverantwortliche von intelligenten Messsystemen müssen ihre vertraulichen Informationen – insbesondere die personenbezogene Informationen - klassifizieren.

a) Die Klassifizierung muss eine eindeutige Abstufung für vertrauliche Informationen besitzen und damit einhergehende Kontrollen zum Schutz der Informationen ausweisen.
b) Die Klassifizierung sämtlicher Informationen muss bei Änderungen im System (zum Beispiel hinzufügen neuer Use Cases) angepasst werden.

Kennzeichnung von Informationen

Control 3.2.2 **Übergreifende Schutzanforderung**

(1) Vertraulich klassifizierte Informationen müssen entsprechend geschützt werden.

a) Zugriffe müssen gemäss Kapitel *Anforderungen an die Zugriffskontrolle* gehandhabt werden.
b) Daten müssen gemäss Kapitel *Anforderungen an das Schlüsselmanagement* verschlüsselt werden.

Control 3.2.3 **Ablese- und Konfigurationsgerät**

(1) Vertraulich klassifizierte Informationen müssen auch hier entsprechend geschützt werden.

a) Vertraulich klassifizierte Daten dürfen auf Ablese- und Konfigurationsgeräten nur verschlüsselt gespeichert werden.
b) Die Devices müssen mindestens mit einem persönlichen PIN/Passwort geschützt werden.
c) Die Devices müssen mit pro Benutzer individuellen Account geschützt werden.
d) Die Geräte müssen einzeln gesperrt werden können z.B. mit Mobile Device Management System.

3.3 Umgang mit Wechseldatenträgern & Telearbeit

Ziel: Sicherstellen, dass der definierte Schutzbedarf der Informationen auf Umsystemen ebenfalls entsprechend umgesetzt wird.

Handhabung von Wechseldatenträgern

Control 3.3.1 **Kommunikationssystem**

(1) Der Datenmanager muss Prozesse für den Umgang mit mobilen Speichermedien (zum Beispiel SIM Karte der intelligenten Messgeräte oder USB-Sticks) definieren.

a) Der Prozess muss freigegeben und angewendet werden.
b) Der Prozess muss einer jährlichen Überprüfung unterzogen werden.

Telearbeit sowie Remote-Support und –Wartung

Control 3.3.2 **Übergreifende Schutzanforderung**

(1) Der Datenmanager muss - sofern umgesetzt - eine Richtlinie sowie zusätzliche Sicherheitsmassnahmen für Telearbeit sowie Remote-Support und -Wartung definieren und einhalten.

a) Die Sicherheitsmassnahmen müssen der Klassifizierung der Informationen und Kritikalität der Systeme, auf die zugegriffen wird, Rechnung tragen.
b) Der Zugriff muss über eine vom Datenmanager kontrollierte resp. auf Sicherheit überprüfte Verbindung erfolgen.
c) Der Zugriff muss verschlüsselt und stark authentisiert sein.
d) Die Sicherheitsmassnahmen müssen den Schutz vor Schadsoftware sowie den Schutz und Erkennung von Angriffen beinhalten.
e) Das berechtigte Auslesen von Daten und nutzen von Funktionen muss protokolliert und kontrolliert werden und der unberechtigte Abfluss von Daten und Nutzung von Funktionen verhindert werden.
f) Der Zugriff von Drittparteien muss weiter auch zeitlich beschränkt sein sowie aufgezeichnet werden.

4. Anforderungen an die Zugriffskontrolle

4.1 Geschäftliche Anforderungen zur Zugriffskontrolle

Ziel: Einschränkung des Zugriffs auf die Assets (Komponenten und Daten).

Zugriffskontrollregelung

Control 4.1.1 **Übergreifende Schutzanforderung**

(1) Der Datenmanager muss ein rollenbasiertes Berechtigungskonzept definieren und umsetzen:

a) Das Need-to-Know Prinzip muss umgesetzt werden. Das bedeutet, dass bei der Steuerung der Zugriffsrechte, jeder Benutzer und jeder Administrator nur auf jene Datenbestände zugreifen und jene Programme ausführen kann, welche für die Arbeit (Aufgabe, Rolle) auch wirklich benötigt wird.

b) Es müssen mindestens die folgenden technischen und nicht technischen Rollen im Konzept sinngemäss definiert und umgesetzt werden:

   I. Administratoren Rollen für Smart Meter, Kommunikationssysteme – insbesondere Datenkonzentrator und Gateway,für das Zähldatenverarbeitungssystem, die Visualisierung sowie die sich darunter befindliche IT Infrastruktur zum Beispiel Server, Datenbanken oder Firewall
   II. Zählerableser lokal
   III. Zählerableser aus der Ferne
   IV. Breaker Manager und Relais Manager
   V. Hersteller Support und Wartung (nach Bedarf)
   VI. Prosumer lokal
   VII. Prosumer Online Visualisierung

c) Sämtliche Verbindungsmöglichkeiten auf die Komponenten (mindestens die vom Hersteller definierte Schnittstellen) müssen in einem dafür vorgesehenen Berechtigungskonzept berücksichtigt werden.

d) Die Gewaltentrennung zwischen Bewilligungsvergabe und Verwaltung von Zugriffsrechten ist nach Möglichkeiten des Datenmanagers zu berücksichtigen.

e) Es muss ein Prozess zur formellen Autorisierung von Berechtigungsanträgen definiert werden

f) Privilegierte Berechtigungen dürfen nur nach einem vordefinierten Prozess vergeben werden. Es ist eine zusätzliche Genehmigungsstufe zu definieren.

g) Berechtigungen müssen nach einem vordefinierten Prozess entzogen werden.

h) Änderungen an Berechtigungen von Benutzer durch Administratoren und automatisch durch Systeme müssen überwacht werden.

i) Das Berechtigungskonzept muss dem Schutzbedarf der Informationen konsistent, über das gesamte intelligente Messsystem Rechnung tragen.

j) Berechtigungen müssen jährlich auf Basis einer Stichprobe überprüft werden.

Control 4.1.2 **Visualisierung**

(1) Das Berechtigungskonzept muss folgende Punkte beachten:

a) Die Endbenutzer Zugriffsberechtigungen auf Daten der Visualisierungsplattform und der lokalen Visualisierung dürfen nicht weniger restriktiv gehalten werden, als bei den anderen Komponenten, auf denen sich diese klassifizierten Daten befinden z.B. Zähldatenverarbeitungssystem. Das gilt für alle Zugriffsarten z.B. via Web App, App oder per proprietäre Devices.
b) Die Endbenutzer Zugriffe müssen protokolliert werden

Zugang zu Netzwerken und Netzwerkdiensten

Control 4.1.3 **Übergreifende Schutzanforderung**

(1) Der Datenmanager muss eine Richtlinie zur Verwendung von Netzwerken und deren Services definieren und umsetzen. Prinzipiell gilt, dass Benutzer nur Zugriff auf Netzwerke und Schnittstellen erhalten, sofern sie dafür vorgängig autorisiert wurden.

a) Insbesondere sind Zugriffe für Telearbeit sowie Remote-Support und Wartungszugriff eingeschränkt und nur gegen entsprechenden Anträge zu vergeben.
b) Die Richtlinie muss definieren:
    I. Welche Netzwerke, Schnittstellen und Services verwendet werden dürfen
    II. Wie der Genehmigungsprozess für diese Netzwerke, Schnittstellen und Services für Benutzer aussieht
    III. Wie die Zugriffe kontrolliert werden
    IV. Wie auf die Netzwerke zugegriffen werden muss
    V. Die zu verwendenden Authentisierungs- und Autorisierungsmechanismen
    VI. Überwachung der Netzwerk Services
    VII. Die Richtlinie für den Gebrauch von Netzwerken, Schnittstellen und deren Services muss mit der Richtlinie für Zugriffskontrollen einhergehen

4.2 Verwaltung des Nutzerzugangs

Control 4.2.1 **Übergreifende Schutzanforderung**

(1) Ein Prozess zur Registrierung von Benutzer (Rollenzuweisung) von intelligenten Messsystemen muss definiert werden, damit die entsprechenden Berechtigungen nachweislich vergeben werden können.

a) Benutzer müssen eindeutig identifizierbar sein (UID).
b) Ausnahme: Die Eindeutigkeit bei der Rolle Zählerableser lokal (read-only) muss nicht zwingend über einen eindeutigen Benutzer erfolgen, sondern kann über das identifizierte Ablese- und Konfigurationsgeräte zum ausschliessen Zweck der Ablesung stattfinden. In diesem Fall muss nachvollziehbar sein, welcher Benutzer, zu welchem Zeitpunkt über das jeweilige Gerät verfügt.

Control 4.2.2 **Smart Meter**

(1) Der Prozess (siehe 4.2.1) muss zudem folgende Punkte beachten:

a) Nicht mehr verwendete UIDs müssen innerhalb eines Monats nach Beendigung des Arbeitsverhältnisses gelöscht werden.
b) Berechtigungen müssen immer in zwei Schritten vergeben bzw. entzogen werden:
    1. UIDs werden erstellt und zugewiesen oder entzogen.

2. Die Berechtigungen (Rollen oder Individualrechte) werden diesen UIDs zugewiesen oder entzogen.

Control 4.2.3 **Visualisierung**

(1) Der Prozess muss weiter folgende Punkte beachten:

a) Nicht mehr verwendete UIDs müssen innerhalb eines Monats nach Beendigung des Vertragsverhältnisses gelöscht werden
b) Berechtigungen müssen immer in zwei Schritten vergeben bzw. entzogen werden:
   1. UIDs werden erstellt und zugewiesen oder entzogen.
   2. Die Berechtigungen werden diesen UIDs zugewiesen oder entzogen.

Vergabe von Zugriffsrechten

Control 4.2.4 **Übergreifende Schutzanforderung**

(1) Benutzerberechtigungen für intelligente Messsysteme dürfen nur gemäss einem vorgängig definierten Prozess vergeben werden.

a) Die Zustimmung des Assetverantwortlichen (gemäss Inventar) ist einzuholen
b) Vergebene Rechte müssen mit der Gewaltentrennung einhergehen.

Control 4.2.5 **Smart Meter**

(1) Der Prozess muss zudem folgende Punkte beachten:

a) Die Benutzerberechtigungen dürfen nicht aktiviert werden, bevor nicht die Zustimmung des Assetverantwortlichen eingeholt und festgehalten wurde.
b) Es muss eine Übersicht von sämtlichen Berechtigungen pro UID existieren.

Control 4.2.6 **Zähldatenverbeitungssystem**

(1) Der Prozess muss weiter folgende Punkte beachten:

a) Die Benutzerberechtigungen dürfen nicht aktiviert werden, bevor nicht die Zustimmung des Assetverantwortlichen eingeholt und festgehalten wurde.
b) Es muss eine Übersicht von sämtlichen Berechtigungen pro UID existieren.

Handhabung privilegierter Zugriffsrechte (gemäss rollenbasiertem Berechtigungskonzept)

Control 4.2.7 **Übergreifende Schutzanforderung**

(1) Die Vergabe von privilegierten Berechtigungen für intelligente Messsysteme muss einer erweiterten Überprüfung unterzogen werden.

a) Dafür muss ein vordefinierter Prozess verwendet werden, der eine zusätzliche Genehmigungsstufe beinhaltet.
b) Für technische Administrations-Konten mit einem generischen Passwort müssen Zugangsdaten durch jährliche Passwort-Änderungen geschützt sein.

c) Mitarbeitende mit privilegierten Berechtigungen müssen eine Geheimhaltungsvereinbarung unterzeichnen, welche ebenfalls den Zeitraum nach Beendigung von Arbeitsverhältnissen abdeckt.
d) Tätigkeiten müssen protokolliert werden

Control 4.2.8 **Smart Meter**

(1) Die erweiterte Überprüfung muss zudem folgende Punkte beachten:

a) Privilegierte Funktionen, müssen identifiziert und entsprechenden Rollen zugeordnet sein. Diesen Rollen müssen definierte Benutzer (UID) zugeordnet werden.
b) Sämtliche privilegierten Rollen müssen durch den Assetverantwortlichen (gemäss Inventar) jährlich (auf Basis einer Stichprobe) überprüft werden.
c) Privilegierte Berechtigungen dürfen nur eindeutig identifizierbaren Benutzern (UID) mit der entsprechenden Rolle vergeben werden, dies gilt auf für technische Benutzer.

Control 4.2.9 **Kommunikationssystem**

(1) Die erweiterte Überprüfung muss zudem folgende Punkte beachten:

a) Privilegierte Funktionen z.B. die Firewall Administration, müssen identifiziert und entsprechenden Rollen zugeordnet sein. Diesen Rollen müssen definierte Benutzer (UID) zugeordnet werden.
b) Sämtliche privilegierten Berechtigungen müssen durch den Assetverantwortlichen (gemäss Inventar) jährlich (auf Basis einer Stichprobe) überprüft werden.

Control 4.2.10 **Zähldatenverarbeitungssystem**

(1) Die erweiterte Überprüfung muss zudem folgende Punkte beachten:

a) Privilegierte Funktionen z.B. zur Datenbank Administration, müssen identifiziert und entsprechenden Rollen zugeordnet sein. Diesen Rollen müssen definierte Benutzer (UID) zugeordnet werden.
b) Sämtliche privilegierten Berechtigungen müssen durch den Assetverantwortlichen (gemäss Inventar) jährlich (auf Basis einer Stichprobe) überprüft werden.
c) Privilegierte Berechtigungen dürfen nur eindeutig identifizierbaren Benutzern (UID) mit der entsprechenden Rolle vergeben werden, dies gilt auf für technische Benutzer.

Control 4.2.11 **Visualisierung**

(1) Die erweiterte Überprüfung muss weiter folgende Punkte beachten:

a) Privilegierte Funktionen z.B. zur Kunden Administration, müssen identifiziert und entsprechenden Rollen zugeordnet sein. Diesen Rollen müssen definierte Benutzer (UID) zugeordnet werden.
b) Sämtliche privilegierten Berechtigungen müssen durch den Assetverantwortlichen (gemäss Inventar) jährlich (auf Basis einer Stichprobe) überprüft werden.
c) Privilegierte Berechtigungen dürfen nur eindeutig identifizierbaren Benutzern (UID) mit der entsprechenden Rolle vergeben werden, dies gilt auf für technische Benutzer.

Handhabung von Passwörtern und Authentisierungsmitteln

Control 4.2.12 **Übergreifende Schutzanforderung**

(1) Die Vergabe von Authentisierungsmitteln für intelligente Messsysteme müssen kontrolliert werden.

a) Passwörter müssen nach der Erst-Anmeldung geändert werden (Diese Massnahme muss technisch erzwungen werden).
b) Passwörter müssen über verschlüsselte Kanäle ausgetauscht werden. Das gilt nicht nur für die Hauptkomponenten, sondern auch für Umsysteme und darunterliegende Plattformen.
c) Benutzer müssen den Erhalt von Zugangsdaten quittieren.
d) Standard-Passwörter von Herstellern / Systemlieferanten müssen bei Erst-Anmeldung geändert werden.
e) Vereinbarungen zur Geheimhaltung von Zugangsdaten müssen von sämtlichen Benutzern unterzeichnet werden.

Überprüfung von Zugriffsrechten

Control 4.2.13 **Übergreifende Schutzanforderung**

(1) Sämtliche Benutzerberechtigungen des intelligenten Messsystems müssen durch den Assetverantwortlichen (gemäss Inventar) jährlich (auf Basis einer Stichprobe) überprüft werden.

a) Sobald sich das Anstellungsverhältnis von Benutzern verändert (Beendigung, Beförderung, Funktionswechsel) müssen die Berechtigungen entsprechend angepasst werden.
b) Änderungen an privilegierten Benutzerkonten müssen protokoliert werden.

Aufhebung oder Anpassung von Zugriffsrechten

Control 4.2.14 **Übergreifende Schutzanforderung**

(1) Zugriffsberechtigungen des intelligenten Messsystems von Benutzern, deren Arbeitsverhältnisse beendet sind, müssen beim Austritt entzogen werden.

a) Zugriffsberechtigungen müssen bereits vor Beendigung des Arbeitsverhältnisses entzogen werden sobald:
    I. Begründeter Verdacht auf Missbrauch besteht
    II. Sich der Benutzer in einer privilegierten Rolle befindet
    III. Die Informationen einen hohen Schutzbedarf ausweisen

4.3 Nutzerverantwortlichkeiten

Ziel: Benutzer sind für den Schutz ihrer Zugangsdaten verantwortlich zu machen.

Nutzung geheimer Zugangsdaten

Control 4.3.1 **Übergreifende Schutzanforderung**

(1) Zugangsdaten für intelligente Messsysteme müssen vertraulich behandelt werden.

a) Passwörter dürfen nur in gesicherten Umgebungen, wie einem Passwort-Safe, aufgezeichnet werden.
b) Bei Verdacht, dass unberechtigte Personen ein Passwort kennen, ist das jeweilige umgehend zu ändern.
c) Passwörter müssen den folgenden Mindestanforderungen entsprechen (dies wird auf den Hauptkomponenten der Systeme bereits von den Herstellern vorgegeben):
    I. Benutzerpasswort müssen mindesten 10 Stellen lang sein.
    II. Trivialpasswörter wie Benutzer-ID, Name, Vorname, Geburtsdatum etc. dürfen nicht verwendet werden.
    III. Passwortwiederholung: Wiederholung nach 10 erfolgten Wechseln
    IV. Fehlversuche: max. 10, anschliessend muss die Benutzer-ID gesperrt werden.
d) Das Passwort ist persönlich und darf nicht weitergegeben werden.
e) Passwörter für automatisierte Log-On Vorgänge müssen den gleichen Sicherheitsvorgaben entsprechen.

4.4 System- und Anwendungszugriffskontrolle

Ziel: Unbefugte Zugriffe auf Assets verhindern.

Sicheres Anmeldeverfahren

Control 4.4.1 **Ablese- und Konfigurationsgeräte**

(1) Der Zugriff auf Ablese- und Konfigurationsgeräte muss durch ein geschütztes Anmeldeverfahren erfolgen.

a) Sollte das Anmeldeverfahren (Log-in) nicht erfolgreich abgeschlossen werden, darf das System keine Auskunft darüber geben, welche Information (Benutzername oder Passwort) nicht korrekt war.
b) Es müssen Sicherheitsmassnahmen implementiert werden, die vor Brute-Force Angriffen schützen.
c) Sowohl erfolgreiche als auch gescheiterte Anmeldeversuche müssen aufgezeichnet werden.
d) Passwörter müssen bei der Eingabe verborgen sein.
e) Passwörter dürfen nicht im Klartext über Netzverbindungen übertragen werden.
f) Systemzugriffssperren müssen nach maximal 15 Minuten automatisch aktiviert werden.

Control 4.4.2 **Smart Meter**

(1) Der Zugriff auf intelligente Messgeräte muss durch ein geschütztes Anmeldeverfahren erfolgen. Für diese Hauptkomponente wird dies vom Hersteller garantiert.

Control 4.4.3 **Kommunikationssystem**

(1) Der Zugriff auf Komponenten des Kommunikationssystems muss durch ein geschütztes Anmeldeverfahren erfolgen. Für diese Hauptkomponente wird dies vom Hersteller garantiert.

Control 4.4.4 **Zähldatenverarbeitungssystem**

(1) Der Zugriff auf Zähldatenverarbeitungssysteme muss durch ein geschütztes Anmeldeverfahren erfolgen. Für den Teil Headendsystem (HES) dieser Hauptkomponente wird dies vom Hersteller garantiert. Für die restlichen Teile und darunterliegenden Plattformen muss folgendes erfolgen:

a) Sollte das Anmeldeverfahren (Log-in) nicht erfolgreich abgeschlossen werden, darf das System keine Auskunft darüber geben, welche Information (Benutzername oder Passwort) nicht korrekt war.
b) Es müssen Sicherheitsmassnahmen implementiert werden, die vor Brute-Force Angriffen schützen.
c) Sowohl erfolgreiche als auch gescheiterte Anmeldeversuche müssen aufgezeichnet werden.
d) Passwörter müssen bei der Eingabe verborgen sein.
e) Passwörter dürfen nicht im Klartext über Netzverbindungen übertragen werden.
f) Systemzugriffssperren müssen nach maximal 15 Minuten automatisch aktiviert werden.

Control 4.4.5 **Visualisierung**

(1) Der Zugriff auf Online Visualisierungen muss durch ein geschütztes Anmeldeverfahren erfolgen.

a) Es dürfen keine sensitiven Informationen dargestellt werden, bevor das Anmeldeverfahren erfolgreich erfolgt ist.
b) Benutzer müssen darauf aufmerksam gemacht werden, dass der Zugriff auf die Informationen nur nach erfolgreicher Autorisierung erfolgen darf.
c) Sollte das Anmeldeverfahren (Log-in) nicht erfolgreich abgeschlossen werden, darf das System keine Auskunft darüber geben, welche Information (Benutzername oder Passwort) nicht korrekt war.
d) Es müssen Sicherheitsmassnahmen implementiert werden, die vor Brute-Force Angriffen schützen.
e) Sowohl erfolgreiche als auch gescheiterte Anmeldeversuche müssen aufgezeichnet werden.
f) Nach erfolgreicher Anmeldung müssen dem Benutzer folgende Informationen angezeigt werden:
    I. Die letzte erfolgreiche Anmeldung
    II. Allfällige nicht erfolgreiche Versuche seit der letzten Anmeldung
g) Passwörter müssen bei der Eingabe verborgen sein.
h) Passwörter dürfen nicht im Klartext über Netzverbindungen übertragen werden.
i) Systemzugriffssperren müssen nach maximal 15 Minuten automatisch aktiviert werden.

Passwort Managementsystem

Control 4.4.6 **Übergreifende Schutzanforderung**

(1) Für die Verwaltung der Passwörter innerhalb des intelligenten Messsystems müssen Passwort Management Systeme verwendet werden. Die Umsysteme und die darunterliegenden Plattformen müssen folgende Kriterien einhalten:

a) Passwörter müssen manuell geändert werden können. Der Prozess muss eine Bestätigung dieser Aktion beinhalten.
b) Passwörter müssen der technischen Richtlinie gemäss Control 4.3.1 entsprechen.
c) Passwörter müssen sicher abgelegt werden.
d) Passwörter müssen nach der Erst-Anmeldung geändert werden.

Nutzung privilegierter Dienstprogramme

Control 4.4.7 **Zähldatenverarbeitungssystem**

(1) Die Verwendung von Unterstützungs-Software auf Zähldatenverarbeitungssystemen (Dienstprogramme) muss eingeschränkt und überwacht werden:

a) Die Verwendung von Dienstprogrammen muss auf ein Minimum eingeschränkt und sollte durch den Hersteller freigegeben werden.
b) Sämtliche nicht benötigten Dienstprogramme müssen deaktiviert oder entfernt werden.
c) Die Verwendung von Dienstprogrammen muss aufgezeichnet werden.
d) Prozesse zur Freigabe von Dienstprogrammen und zu deren Sperrung nach Gebrauch müssen formell dokumentiert und freigegeben sein.

5. Anforderungen an das Schlüsselmanagement

5.1 Kryptografische Kontrollmassnahmen

Ziel: Sicherzustellen, dass kryptografische Massnahmen auf korrekte und wirksame Weise zum Schutz der Verschlüsselung und somit der Vertraulichkeit von Personen- und Profildaten, der Authentizität von Systemen und der Integrität von Informationen und Funktionen einsetzt werden.

Schlüsselmanagement

Control 5.1.1 **Übergreifende Schutzanforderung**

(1) Die Verwendung und der Schutz von kryptographischen Schlüsseln innerhalb intelligenter Messsysteme muss gemäss einer vordefinierten Richtlinie erfolgen.

a) Die Richtlinie adressiert das Schlüsselmanagement des iMS während des gesamten Lebenszyklus aller kryptografischen Schlüssel. Dies von der Generierung über die Verteilung bis zur Sperrung.
b) Die Richtlinien müssen freigegeben und angewendet werden sowie einer jährlichen Überprüfung unterzogen werden.
c) Die Richtlinie muss konkret folgende Themen definieren:
    I. Generieren von kryptographischen Schlüsselmaterial für die definierten Anwendungsbereiche
    II. Verwendung von PKI Zertifikaten. Die Gesamtheit der in einem iMS befindlichen Schlüssel muss durch ein Schlüsselmanagement verwaltet werden.
    III. Sichere Verteilung der generierten Schlüssel und deren Aktivierung. Diese kann lokal oder via Fernwartung erfolgen.
    IV. Geeignete Sicherheitsfunktionen zum Schutz gegen unautorisierten Zugriff auf Schlüsselmaterial sind implementiert. Der Schlüssel muss so abgelegt sein, dass er vor der Aktivierung nicht ausgelesen werden kann.
    V. Prozesse zur Änderung von kryptographischen Schlüsseln
    VI. Umgang mit kompromittierten Schlüsseln
    VII. Deaktivierung von kryptographischen Schlüsseln
    VIII. Wiederbeschaffung von verlorenen / korrupten Schlüsseln
    IX. Archivierung von kryptographischen Schlüsseln
    X. Vernichtung von nicht mehr benötigten Schlüsseln
    XI. Aufzeichnung von Aktivitäten innerhalb des Key Management Systems
    XII. Nebst dem Umgang mit privaten Schlüsseln, muss ebenfalls die Zusammenarbeit mit Herstellern / Systemlieferanten von öffentlichen Schlüsseln definiert werden.
    XIII. Vorinstalliertes Schlüsselmaterial des Lieferanten auf Hauptkomponenten bzw. anderen Zählern dient ausschliesslich der Inbetriebnahme, darf im Betrieb nicht angewendet werden und wird bei der Inbetriebnahme durch operativ anzuwendende Schlüssel ersetzt.

6. Anforderungen an die physische und gerätebezogene Sicherheit

6.1 Gesicherte Bereiche

Ziel: Unbefugten physischen Zugang verhindern, um Schäden und Eingriffe an Assets abzuwenden.

Physische Zutrittskontrollmassnahmen

Control 6.1.1 **Übergreifende Schutzanforderung**

(1) Der physische Zugang in denen sich kritische Informationen befinden (bspw. Datenkonzentratoren), muss durch Sicherheitskontrollen eingeschränkt werden.

Control 6.1.2 **Zähldatenverarbeitungssystem**

(1) Zähldatenverarbeitungssysteme müssen sich in geschützten Bereichen befinden, welche vor Unberechtigten geschützt werden.

a) Die Zutrittskontrolle muss aus einer starken Authentisierung bestehen wie zum Beispiel aus Zutrittskarte (Batch).
b) Der Zutritt für externe Support-Mitarbeitende muss eingeschränkt, autorisiert sowie protokolliert werden.
c) Sämtliche Zutritts-Berechtigungen für Datacenters und Betriebszentralen müssen jährlich (auf Basis einer Stichprobe) überprüft und angepasst werden.

Control 6.1.3 **Visualisierung**

(1) Online Visualisierungssysteme müssen sich in geschützten Bereichen befinden, welche vor Unberechtigten geschützt werden.

a) Die Zutrittskontrolle muss aus einer starken Authentisierung bestehen wie zum Beispiel aus Zutrittskarte (Batch).
b) Der Zutritt für externe Support-Mitarbeitende muss eingeschränkt, autorisiert sowie protokolliert werden.
c) Sämtliche Zutritts-Berechtigungen für Datacenters und Betriebszentralen müssen jährlich (auf Basis einer Stichprobe) überprüft werden.

6.2 Geräte

Ziel: Schäden, Betriebsstörungen, Diebstahl oder Kompromittierung von Assets verhindern.

Control 6.2.1 **Smart Meter**

(1) Der Datenmanager stellt sicher, dass während des Installationsprozesses die Smart Meter nicht manipuliert werden können.

Gerätewartung

Control 6.2.2 **Übergreifende Schutzanforderung**

(1) Intelligente Messsysteme müssen regelmässig gewartet werden, damit deren Vertraulichkeit und Integrität sichergestellt ist.

a) Angaben von Herstellern zu Wartungsintervallen, Wartungsanforderungen und Wartungsumfang müssen berücksichtigt werden.
b) Wartungsarbeiten dürfen ausschliesslich von dafür ausgebildeten Personen durchgeführt werden.
c) Präventive und korrigierende Wartungen und damit verbundene Fehler müssen dokumentiert werden.
d) Werden Komponenten von intelligenten Messsystemen durch externe Mitarbeitende gewartet, müssen vorgelagerte Kontrollen sicherstellen, dass sich keine kritischen Informationen mehr auf dem Gerät befinden.
e) Geräte müssen nach der Wartung auf allfällige Fehlkonfigurationen überprüft werden, bevor sie wiedereingesetzt werden.
f) Dies gilt auch bei der Installation und Inbetriebnahme des intelligenten Messgerätes.

Entfernen von Assets

Control 6.2.3 **Übergreifende Schutzanforderung**

(1) Komponenten und Informationen von intelligenten Messsystemen dürfen nicht ohne vorgängige Genehmigung entfernt werden z.B. für Wartungszwecke.

a) Mitarbeitende (inklusive Externe), die berechtigt sind, Informationen und Komponenten von intelligenten Messsystemen mitzuführen, müssen identifiziert und instruiert sein.
b) Es muss der Zeitpunkt dokumentiert werden, an dem die Komponenten:
    I. entfernt werden
    II. retourniert worden sind.

Sichere Entsorgung oder Wiederverwendung von Geräten

Control 6.2.4 **Übergreifende Schutzanforderung**

(1) Vor der Entsorgung von Komponenten muss überprüft werden, dass sich keine sensitiven Informationen auf den Speichermedien befinden.

a) Prozesse müssen freigegeben und angewendet werden sowie einer jährlichen Überprüfung unterzogen werden.
b) Daten mit Schutzbedarf, die auf Datenträgern gespeichert wurden, werden durch ein Verfahren nach Stand der Technik unlesbar gemacht. Persistente Datenträger werden gemäss diesen Anforderungen unlesbar gemacht.

7. Anforderungen an den sicheren ICT Betrieb

7.1 Betriebliche Verfahren und Verantwortlichkeiten

Ziel: Den korrekten und sicheren Betrieb des intelligenten Messsystems sicherstellen.

Change Management

Control 7.1.1 **Übergreifende Schutzanforderung**

(1) Veränderungen an Prozessen und den Komponenten des intelligenten Messsystems müssen kontrolliert werden.

a) Signifikante Änderungen müssen aufgezeichnet werden.
b) Bevor Änderungen in die Produktion übernommen werden, muss deren Auswirkung auf die Informationssicherheit und auf die Konformität der Hauptkomponenten beurteilt werden.
c) Das Change-Management muss Genehmigungsprozesse vorsehen.
d) Das Change-Management muss Fall-Back Prozesse und Verantwortlichkeiten definieren, die im Falle eines nicht erfolgreichen Changes vom Datenmanager eingesetzt werden können.

Trennung von Entwicklungs-, Test- und betriebsfähigem Umfeld

Control 7.1.2 **Übergreifende Sicherheitsanforderung**

(1) Die produktiven Umgebungen müssen von Test- und Integrationsumgebung getrennt werden.

a) Änderungen an Systemen müssen zuerst in der Test-Umgebung getestet werden, bevor die Änderung in der produktiven Instanz implementiert wird.
b) Sensitive Daten - insbesondere personenbezogene Daten - dürfen nur in die Test Umgebung integriert werden, wenn gleichwertige Sicherheitskontrollen vorherrschen oder die Daten anonymisiert wurden

7.2 Schutz vor Angriffen und Schadsoftware

Ziel: Den Schutz des intelligenten Messsystems vor Angriffen und Schadsoftware sicherzustellen.

Präventive und detektiven Schutzmassnahmen

Control 7.2.1 **Übergreifende Schutzanforderung**

(1) Das intelligente Messsystem muss mit Hilfe von präventiven und detektiven Massnahmen geschützt werden.

a) Benutzer müssen mindestens alle drei Jahre durch geeignete Awareness-Massnahmen geschult werden.
b) Der Datenmanager muss regelmässig Informationen über, Schwachstellen und konkrete Bedrohungen der verwendeten Komponenten / Technologien von vertrauenswürdigen Quellen sowie den Herstellern zusammentragen und auswerten.

c) Informationen und Meldungen über potentielle Schwachstellen müssen durch vordefinierte Prozesse verifiziert werden.
d) Es müssen Prozesse und Verantwortlichkeiten für den Umgang mit Schadsoftware und Angriffen definiert werden. Dazu gehören die korrekte Verwendung der Schutzmechanismen sowie die Reaktion auf Schadsoftware und Angriffe.

Control 7.2.2 **Smart Meter**

(1) Intelligente Messgeräte müssen mit Hilfe von detektiven Massnahmen geschützt werden.

a) Smart Meter müssen auf nicht autorisierte Dateien, Prozesse und Kommunikationsverbindungen überprüft werden. Dabei entdeckte Änderungen müssen analysiert und mit dem Hersteller korrigiert werden.

Control 7.2.3 **Kommunikationssysteme**

(1) Kommunikationssysteme müssen mit Hilfe von detektiven Massnahmen auch in der Mitverantwortung des Datenmanagers geschützt werden.

a) Die Systeme müssen auf nicht autorisierte Dateien, Prozesse und Kommunikationsverbindungen überprüft werden. Dabei entdeckte Änderungen müssen analysiert und vom Hersteller korrigiert werden.

Control 7.2.4 **Zähldatenverarbeitungssystem**

(1) Zähldatenverarbeitungssysteme müssen mit Hilfe von präventiven und detektiven Massnahmen geschützt werden.

a) Die Verwendung von nicht autorisierter Software muss mittels geeigneter Kontrollen (Whitelisting) verhindert werden.
b) Die Verwendung von unsicheren Services und Downloads muss mittels geeigneter Kontrollen verhindert werden (Firewalling).
c) Die Systeme müssen auf nicht autorisierte Dateien, Prozesse und Kommunikationsverbindungen überprüft werden. Dabei entdeckte Änderungen müssen analysiert und vom Datenmanager oder Hersteller korrigiert werden.
d) Es müssen Antivirus-Lösungen installiert und regelmässig aktualisiert werden.

Control 7.2.5 **Visualisierungen**

(1) Die entfernte Visualisierung muss mit Hilfe von präventiven und detektiven Massnahmen geschützt werden.

a) Die Verwendung von nicht autorisierter Software muss mittels geeigneter Kontrollen (Whitelisting) verhindert werden.
b) Die Verwendung von unsicherem Web Services muss mittels geeigneter Kontrollen verhindert werden u.a. Web Applikation Firewall.
c) Die Systeme auf nicht autorisierte Dateien, Prozesse und Kommunikationsverbindungen überprüft werden. Dabei entdeckte Änderungen müssen analysiert und korrigiert werden.

7.3 Backup und Recovery

Ziel: Eine angemessene Sicherung und Wiederherstellung von Systemen, Applikationen, Konfigurationen und Daten zum Schutz vor Verlust und zur Sicherstellung einer zeitnahen Wiederherstellung

Control 7.3.1 **Übergeordnete Anforderung**

(1) Ein Prozess für das Backup und Recovery muss definiert sein.

a) Der Prozess muss Backup und Recovery Verfahren für Informationen, Software, Systemen, Konfigurationen und Schlüssel definieren.
b) Aufbewahrungsdauer und Sicherheitsanforderungen müssen definiert sein und den gesetzlichen Anforderungen entsprechen.
c) Recovery Tests sind regelmässig durchzuführen.

7.4 Aufzeichnung und Überwachung

Ziel: Die Identifikation von sicherheitsrelevanten Ereignissen muss sichergestellt sein, um auf Ereignisse zeitnahe reagieren zu können.

Ereignis-Protokollierung

Control 7.4.1 **Smart Meter**

(1) Für intelligente Messgeräte muss das Sicherheitsprotokoll aktiviert sein, dass sowohl Zeitpunkt, Kennung (UID) des Benutzers bzw. Systems, die betroffene Schnittstelle sowie das Ereignis aufzeichnet. Folgende Ereignisse müssen in dieser Form aufgezeichnet werden:

a) Verwendung von Benutzerberechtigungen
b) Erfolgreiche und gescheiterte Updates von Software
c) Erfolgreiche und gescheiterte Authentisierung
d) lokale Anmeldeversuche
e) Konfigurationsänderungen
f) Änderungen an Berechtigungen
g) Verbindungsaufbau
h) physische Manipulation
i) und weitere sicherheitsrelevante Ereignisse

Control 7.4.2 **Zähldatenverarbeitungssystem**

(1) Für die Zähldatenverarbeitungssysteme muss das Sicherheitsprotokoll aktiviert sein, das sowohl Zeitpunkt, Kennung (UID) des Benutzers bzw. Systems, die betroffene Schnittstelle sowie das Ereignis aufzeichnet. Folgende Ereignisse müssen in dieser Form aufgezeichnet werden:

a) Verwendung von erhöhten Benutzerberechtigungen u.a. Breaker Funktion
b) Erfolgreiche und gescheiterte Updates von Software
c) Erfolgreiche und gescheiterte Authentisierung
d) lokale Anmeldeversuche
e) Konfigurationsänderungen
f) Änderungen an Berechtigungen
g) Verbindungsaufbau
h) und weitere sicherheitsrelevante Ereignisse

Control 7.4.3 **Visualisierung**

(1) Für die Visualisierungsplattform muss das Sicherheitsprotokoll aktiviert sein, das sowohl Zeitpunkt, Kennung (UID) des Benutzers bzw. Systems, die betroffene Schnittstelle sowie das Ereignis aufzeichnet. Folgende Ereignisse müssen in dieser Form aufgezeichnet werden:

a) Erfolgreiche und gescheiterte Authentisierung
b) Konfigurationsänderungen
c) Änderungen an Berechtigungen
d) und weitere sicherheitsrelevante Ereignisse

Schutz der Protokollinformationen

Control 7.4.4 **Smart Meter**

(1) Die Protokolle müssen vor unbefugten Veränderungen geschützt sein.

a) Log-Daten dürfen nur durch entsprechend autorisierte Benutzer ausgelesen werden.
b) Log Dateien dürfen nur durch autorisierte Aktionen verändert oder gelöscht werden.

Control 7.4.5 **Zähldatenverarbeitungssystem**

(1) Die Protokolle müssen vor unbefugten Veränderungen geschützt sein.

a) Log-Daten dürfen nur durch entsprechend autorisierte Benutzer ausgelesen werden.
b) Log Dateien dürfen nur durch autorisierte Aktionen verändert oder gelöscht werden.

Control 7.4.6 **Visualisierung**

(1) Die Protokolle müssen vor unbefugten Veränderungen geschützt sein.

a) Log-Daten dürfen nur durch entsprechend autorisierte Benutzer ausgelesen werden.
b) Log Dateien dürfen nur durch autorisierte Aktionen verändert oder gelöscht werden.

7.5 Kontrolle der betrieblichen Software

Ziel: Die Integrität im Betrieb des intelligenten Messsystems sicherzustellen.

Installation von Software auf betrieblichen Systemen

Control 7.5.1 **Smart Meter**

(1) Die Installation von Firmware auf intelligente Messgeräten muss überwacht werden. Zu diesem Zweck müssen Prozesse formell dokumentiert und freigegeben sein. Die folgenden Punkte sind abzudecken:

a) Firmware Updates dürfen nur durch qualifizierte Administratoren mit vorgängig eingeholter Genehmigung durchgeführt werden.
b) Firmware darf erst implementiert werden, sobald diese gemäss Change-Management Prozessen auf einem separaten Testsystem getestet wurde.
c) Zum Schutz von Konfigurationen und Dokumentationen muss ein Versionen Kontroll-System verwendet werden.
d) Bevor Changes auf produktive Geräte gespielt werden, muss eine Rollback Strategie definiert sein.
e) Vorgängige Versionen der Firmware müssen als Fall-Back-Massnahme aufbewahrt werden.
f) Ein Audit Log für sämtliche Changes, die in die Produktion gespielt wurden, ist zu führen.
g) Bevor ein Upgrade der Firmware durchgeführt wird, müssen sowohl die betrieblichen Anforderungen als auch die Auswirkung auf die Informationssicherheit mit dem Hersteller geprüft werden.

Control 7.5.2 **Zähldatenverarbeitungssystem**

(1) Die Installation von Software sowie Betriebssystemen auf intelligenten Zähldatenverarbeitungssystemen muss überwacht werden. Zu diesem Zweck müssen Prozesse formell dokumentiert und freigegeben sein, die folgende Punkte abdecken.

a) Software Updates dürfen nur durch qualifizierte Administratoren mit vorgängig eingeholter Genehmigung durchgeführt werden.
b) Software darf erst implementiert werden, sobald diese gemäss Change-Management Prozessen auf einem separaten Testsystem getestet wurde.

7.6 Management technischer Schwachstellen

Ziel: Die Ausnutzung technischer Schwachstellen verhindern.

Management technischer Schwachstellen

Control 7.6.1 **Übergreifendes Schutzobjekt**

(1) Es muss eine aktive Überwachung und Prüfung von Informationen über potentielle Schwachstellen innerhalb der intelligenten Messgeräte durch den Hersteller und den Datenmanager erfolgen.

a) Sobald eine Schwachstelle identifiziert wurde, muss das damit einhergehende Risiko beurteilt und entsprechende Patches installiert werden. Steht noch kein Patch zur Verfügung, so müssen alternative Sicherheitsmassnahmen in Betracht gezogen und nach Möglichkeit umgesetzt werden.
b) Die geeignete Kommunikationsstrategie bei Sicherheitsschwachstellen muss definiert sein.
c) Der Betreiber hat zu verifizieren, dass der Lieferant qualifiziertes Vulnerability- und Patchmanagementprozesse pflegt.

Einschränkungen im Hinblick auf die Installation von Software

Control 7.6.2 **Smart Meter**

(1) Auf dem intelligenten Messgerät dürfen nur die im aktuellen Use Case, zur Aufgabenerfüllung entsprechenden und erforderliche Minimalkonfiguration und Funktionen, aktiviert sein.

Control 7.6.3 **Zähldatenverarbeitungssystem**

(1) Auf dem Zähldatenverarbeitungssystem darf nur die zu seiner Aufgabenerfüllung erforderliche Software installiert sein.

8. Anforderungen an die Kommunikationssicherheit

8.1 Netzwerksicherheitsmanagement

Ziel: Den Schutz der Verfügbarkeit und der Integrität von Kommunikationssystemen sicherstellen.

Netzwerksicherheitsmassnahmen

Control 8.1.1 **Übergreifende Schutzanforderung**

(1) Der Datenmanager und dessen Dienstleister müssen sicherstellen, dass ihre Netzwerke oder Netzwerkdienste von unberechtigten Zugriffen geschützt werden.

a) Prozesse und Verantwortlichkeiten für die Verwaltung von Netzwerkgeräten müssen definiert sein.
b) Verantwortlichkeiten für Netzwerke und Betrieb von Gerätschaften müssen nach Möglichkeit getrennt werden.
c) Es müssen dedizierte Kontrollen zum Schutz der Vertraulichkeit und Integrität von Informationen implementiert werden, die über öffentliche Netzwerke oder Wireless Protokolle gesendet werden (dies gilt für die Umsysteme – bei den Hauptkomponenten muss dies per Design gewährleistet sein).
d) Für die Informationssicherheit relevante Events müssen aufgezeichnet und überwacht werden (Logging & Monitoring).
e) Umsysteme müssen sich am Netzwerk authentisieren.
f) Die Verbindung zum Netzwerk für Komponenten, welche nicht dem iMS dienen, müssen eingeschränkt sein.

Sicherheit von Netzwerkdiensten

Control 8.1.2 **Übergreifende Schutzanforderung**

(1) Alle spezifizierten Schnittstellen des intelligenten Messsystems dürfen nur für die Funktionalitäten eingesetzt werden für welche diese bestimmt sind.

a) Die Verwendung der Schnittstellen muss überwacht werden.

Control 8.1.3 **Kommunikationssystem**

(1) Kommunikationsdienste und deren Erfüllungsgrad - im speziellen für Sicherheitsdienste - müssen überwacht werden, unabhängig davon, ob der der Dienst selbst oder durch Dritte erbracht wird. Zu den Sicherheitsdiensten gehören:

a) Dienste für Authentisierung, Verschlüsselung und Zugriffskontrollen
b) Technische Parameter für die gesicherten Verbindungen zum Provider

Segmentierung von Netzwerken

Control 8.1.4 **Übergreifende Schutzanforderung**

(1) Die Netzwerke müssen segmentiert sein:

a) Innerhalb des Backends des Datenmanagers müssen sich die Hauptkomponenten insbesondere das HES in von der Visualisierung und von Clients abgetrennten Segmenten befinden.

8.2 Informationstransfer

Ziel: Die Sicherheit der Informationen aufrechterhalten, welche mit externen Systemen ausgetauscht werden.

Regelungen und Verfahren zum Informationstransfer

Control 8.2.1 **Übergreifende Schutzanforderung**

(1) Zur Übertragung von Informationen zu externen Systemen müssen Kontrollen implementiert werden:

a) Der Datenverkehr erfolgt verschlüsselt um den Schutz der zu übertragenden Informationen vor Abfangen durch Dritte, Kopieren, Änderung sowie Zerstörung zu gewährleisten.
b) Informationen, die über öffentliche Netzwerke ausgetauscht werden, müssen mittels Datenverschlüsselung oder mittels einer Absicherung der Datenverbindung abgesichert werden. Dabei muss folgendes beachtet werden:
    I. Sämtliche Kommunikationspartner müssen berücksichtigt werden.
    II. Der Austausch benötigter Schlüssel muss durch einen vordefinierten Prozess erfolgen.

9. Anforderungen an die Systemlieferantenbeziehungen

9.1 Informationssicherheit in Systemlieferantenbeziehungen

Behandlung von Sicherheitsfragen in Systemlieferantenvereinbarungen

Control 9.1.1 **Übergreifende Schutzanforderung**

(1) Mit externen Leistungserbringern, welche intelligente Messgeräte betreiben, supporten oder warten, müssen Sicherheitsabmachungen formal festgelegt und in Liefervereinbarungen dokumentiert werden.

a) Die Sicherheitsabmachungen müssen die rechtlichen Anforderungen, insbesondere die Datenschutzanforderungen erfüllen.
b) Die Sicherheitsabmachungen müssen die regulatorischen Anforderungen (insbesondere die hier vorliegenden Anforderungen) erfüllen.
c) Es muss festgelegt werden, wie der externe Leistungserbringer diese Anforderungen erfüllt.
d) Die Vereinbarung muss sämtliche Personen des externen Leistungserbringers auflisten, welche Zugriff auf die kritischen Daten oder die Hauptkomponenten erhalten und beschreiben, welche (Sicherheits-) Anforderungen an die Personen gestellt werden, damit diese den Zugriff auf die Informationen enthalten.
e) Die Vereinbarung muss Kontaktpersonen definieren, die im Falle von Sicherheitsvorfällen zu kontaktieren sind.
f) Die Vereinbarung muss definieren, dass der Datenmanager das Recht hat, die definierten Sicherheitsanforderungen beim externen Leistungserbringer zu überprüfen (Auditrecht).
g) Der externe Leistungserbringer muss dazu verpflichtet werden, die Sicherheitsanforderungen vom Hersteller oder Datenmanager von Komponenten des Kommunikationssystems einzuhalten.

9.2 Management der Erbringung von Dienstleistungen durch Systemlieferanten

Ziel: Sicherstellung, dass die Lieferanten ihre Verpflichtungen wahrnehmen

Überwachung und Überprüfung von Systemlieferantendienstleistungen

Control 9.2.1 **Übergreifende Schutzanforderung**

(1) Die von externen Leistungserbringern und allfälligen Unterlieferanten gelieferten Dienstleistungen müssen überwacht und jährlich überprüft werden. Damit sind nicht die zertifizierten Hauptkomponenten gemeint.

a) Innerhalb dieser Überprüfung muss der externe Leistungserbringer Informationen über allfällige Sicherheitsvorfälle offenlegen. Diese Informationen müssen gemäss den definierten Sicherheitsanforderungen überprüft werden.
b) Bei der Überprüfung festgestellte Probleme müssen gelöst und überwacht werden.

10. Anforderungen an das Management von Informationssicherheitsvorfällen

10.1 Management von Informationssicherheitsvorfällen und –Verbesserungen

Ziel: Eine konsistente und effektive Vorgehensweise im Hinblick auf die Handhabung von Sicherheitsvorfällen sicherzustellen, einschliesslich der Meldung von Sicherheitsereignissen und Schwachstellen.

Verantwortlichkeiten und Verfahren

Control 10.1.1 **Übergreifende Schutzanforderung**

(1) Für eine schnelle sowie effiziente Reaktion auf allfällige Sicherheitsvorfälle müssen Verantwortlichkeiten sowie Prozesse definiert sein.

a) Prozesse müssen freigegeben und angewendet werden sowie einer jährlichen Überprüfung unterzogen werden.

Meldung von Informationssicherheitsereignissen

Control 10.1.2 **Übergreifende Schutzanforderung**

(1) Sicherheitsvorfälle insbesondere Datendiebstahl, Manipulationen oder sicherheitsbedingte Ausfälle des iMS müssen an die Geschäftsleitung sowie an externe Anspruchsgruppen (z.B. MELANI oder Kantonaler Datenschutzbeauftragter) gemeldet werden.

a) Zu diesem Zweck müssen die entsprechenden Prozesse und Verantwortlichkeiten sowie Kontaktpersonen vorgängig definiert sein.

Meldung von Schwachstellen in der Informationssicherheit

Control 10.1.3 **Übergreifende Schutzanforderung**

(1) Mitarbeitende des Datenmanagers müssen allfällige Schwachstellen am iMS melden.

a) Für die Meldung solcher Schwachstellen muss eine Kontaktperson und ein übersichtlicher bzw. effizienter Prozess definiert werden.

Reaktion auf Informationssicherheitsvorfälle

Control 10.1.4 **Übergreifende Schutzanforderung**

(1) Die Reaktion auf Sicherheitsvorfälle muss anhand vorgängig definierter Prozesse erfolgen.

a) Wiederherstellungspläne müssen vorbereitet werden, um in Fällen von Schadsoftware und Angriffen angemessen reagieren zu können.

11. Compliance Anforderungen

11.1 Compliance im Hinblick auf rechtliche und vertragliche Anforderungen

Ziel: Vermeidung von Verstössen gegen rechtliche, regulatorische oder vertragliche Verpflichtungen im Hinblick auf die Informationssicherheit und jegliche anderweitigen Sicherheitsanforderungen.

Schutz vor Aufzeichnungen

Control 11.1.1 **Übergreifende Schutzanforderung**

(1) Informationen aus intelligenten Messsystemen müssen vor unautorisierten Zugriffen sowie Veröffentlichung, Zerstörung und Verlust geschützt werden.

a) Dafür implementierte Schutzmechanismen müssen sowohl die Klassifizierung der Informationen sowie rechtliche als auch regulatorische Auflagen berücksichtigen.

Datenschutz und Schutz personenbezogener identifizierbarer Informationen

Control 11.1.2 **Übergreifende Schutzanforderung**

(1) Der Schutz der personenidentifizierenden Daten muss komplementär zu den in diesem Dokument aufgeführten Anforderungen gemäss datenschutzrechtlichen Vorgaben erfolgen.

11.2 Überprüfung der Informationssicherheit

Ziel: Sicherstellen, dass die Informationssicherheit gemäss den regulatorischen und internen Vorgaben durchgeführt und betrieben wird.

Technische Compliance-Überprüfung

Control 11.2.1 **Übergreifende Schutzanforderung**

(1) Der Datenmanager muss eine jährliche technische Überprüfung (auf Basis einer Stichprobe) der intelligenten Messsysteme durchführen, um festzustellen, ob diese den regulatorischen und internen Vorgaben entsprechen z.B. ob die Sicherheitskonfigurationen den Vorgaben und Best Practises entsprechen.

a) Die Überprüfung muss - sofern umsetzbar - automatisiert erfolgen. Manuelle Überprüfungen dürfen nur von qualifizierten System-Ingenieuren und Security Experten durchgeführt werden.