Informationssicherheit

Richtlinie
für Dienstleister und Lieferanten

ENERVIE – Südwestfalen Energie und Wasser AG
Finanzen/ Einkauf/ IT
Informationssicherheit

Platz der Impulse 1
58093 Hagen

Klassifizierung: Intern

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	Bearbeitet durch	Änderung
0.1	14.07.2020	Klahr	Initiale Erstellung
1.0	12.10.2020	Klahr	Finalisierung

Prüfung

Version	Datum	Geprüft durch	Änderung
1.0	12.10.2020	Klahr	Finalisierung

Freigabe und Klassifizierung

Version	Datum	Klassifizierung	Freigegeben und klassifiziert durch
1.0	12.10.2020	Öffentlich	Klahr

Ersteller	Klahr
Besitzer	Informationssicherheit ENERVIE

Einleitung

Die ENERVIE Südwestfalen Energie und Wasser AG und deren Tochterunternehmen (im folgendem ENERVIE genannt) ist sich der Bedeutung der bei ihr verarbeiteten Informationen im Rahmen ihrer gesetzlichen Anforderungen und unter Berücksichtigung ihrer Geschäftsziele bewusst. Um ihre Informationen zu schützen und ihre Geschäftsziele zu verwirklichen, sorgt die ENERVIE in allen Bereichen für eine angemessene Sicherheit ihrer Informationswerte.
Zur Einhaltung der notwendigen Informationssicherheitsstandards innerhalb der ENERVIE vereinbaren die Parteien in Ergänzung zu den allgemeinen Einkaufsbedingungen die hier folgenden Anforderungen an den Auftragnehmer zur Informationssicherheit.

1 Anwendungsbereich

Diese Richtlinie ist gültig für Auftragnehmer der ENERVIE, die im Rahmen eines Vertragsverhältnisses Zutritt zu Gebäuden oder Räumlichkeiten, Zugang und/oder Zugriff auf elektronische Informationen oder Informationssysteme der ENERVIE erhalten.
Der Auftragnehmer sorgt innerhalb seines Unternehmens für die Bekanntmachung dieser Sicherheitsrichtlinie, werden durch den Auftragnehmer Dritte zur Erfüllung der Aufgaben im Rahmen des Auftrages eingesetzt, so sind dieses ENERVIE zu benennen und durch ENERVIE zu genehmigen. Die Regelungen dieser Vereinbarung sind auch für Subunternehmer des Auftragnehmers bindend.

2 Vertraulichkeit

Jeder Auftragnehmer der ENERVIE ist verpflichtet, sämtliche Informationen, die er im Zusammenhang mit der Tätigkeit erhält oder ihm zugänglich sind, streng vertraulich zu behandeln, sie insbesondere keinem Dritten zu offenbaren oder für andere als bestimmungsgemäße Zwecke zu verwenden. Der Auftragnehmer hat bei Beendigung der Beauftragung erhaltene Unterlagen unaufgefordert sicher zu vernichten oder auf Verlangen zurückzugeben. Von der ENERVIE erhaltene Schlüssel, Zutritts-/Zugangskarten und –token, sowie Endgeräte sind unverzüglich und unaufgefordert zurückzugeben. Die Verpflichtung zur Vertraulichkeit besteht über die jeweilige Zusammenarbeit hinaus auf Dauer fort.

3 Personalsicherheit

Der Auftragnehmer benennt der ENERVIE einen Ansprechpartner für Informationssicherheit der für die Umsetzung, Aufrechthaltung und Überprüfung der Informationssicherheitsmaßnahmen verantwortlich ist. Der Auftragnehmer beschäftigt ausschließlich vertrauenswürdiges Personal, dass im Umgang mit Informationswerten in Datenschutz und Informationssicherheit geschult wurde. Als vertrauenswürdiges Personal ist Personal definiert, welches vom Auftragnehmer nach geltendem Recht und geschäftlichen Anforderungen überprüft wurde. Scheiden relevante Mitarbeiter des Auftragnehmers aus dem Unternehmen aus oder sind nicht mehr mit Tätigkeiten im Rahmen des Auftrages betraut, so ist durch geeignete Maßnahmen sicherzustellen, dass Zutritts-, Zugangs- und Zugriffs-Berechtigungen entzogen werden und die Informationswerte der ENERVIE unbeeinträchtigt geschützt bleiben. Das Ausscheiden von Mitarbeitern des Auftragnehmers die Zutritts-, Zugangs- und/oder Zugriffs-Berechtigungen besessen haben, ist der ENERVIE anzuzeigen.

4 Störungen, Ereignisse und Vorfälle der Informationssicherheit

Störungen der Informationstechnologien behindern Arbeitsabläufe, meistens beruht eine Störung auf einer überschaubaren Beeinträchtigung der Verfügbarkeit von Daten. Von einem Ereignis der Informationssicherheit spricht man, wenn der Verdacht besteht, dass Vertraulichkeit oder Integrität von Informationen gefährdet sind oder eine Beeinträchtigung der Verfügbarkeit längerfristig anstehen könnte. Bei einem Vorfall der Informationssicherheit wurden bereits die Vertraulichkeit oder Integrität von Informationen verletzt oder die Verfügbarkeit ist bereits längerfristig beeinträchtigt. Ereignisse und Vorfälle sind erhebliche Störungen, die bei Nicht-Behandlung zu immer weiterführenden negativen Auswirkungen führen und einen hohen finanziellen Schaden verursachen können. Der Auftragnehmer ist verpflichtet, die oben beschriebenen Beeinträchtigungen in seiner Organisation, die potenziell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Informationswerte des Auftraggebers haben könnten, umgehend ohne Zeitverzug dem im Vertrag benannten Ansprechpartner auf Seiten des Auftraggebers zu melden. Der Auftragnehmer wird im Falle eines Vorfalls Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitstellen.

5 Dokumentation

Der Auftragnehmer ist verpflichtet, eine Dokumentation zur Verfügung zu stellen, die die Nutzung der angebotenen Lösung unterstützt. Der gebräuchliche Umfang einer derartigen Dokumentation, wenn auch nicht auf diese beschränkt, inkludiert die folgenden Punkte:

- Liste der Hardware
- Liste der Software (inklusive Betriebssystem und Patch-Level)
- Übersichtsplan der Systemarchitektur
- Kommunikationsmatrix und Schnittstellendarstellung
- Existierende Benutzerkonten und Rollen sowie deren Berechtigungen
- Beschreibung der grundlegenden Funktionen und Prozesse
- Beschreibung von Sicherheitsmechanismen

Sollten Änderungen an der gelieferten Lösung durchgeführt werden, wird vom Auftragnehmer erwartet, diese in die Dokumentation einzupflegen.

6 Einsatz kryptographischer Lösungen

Der Auftragnehmer muss sicherstellen, dass der Einsatz der kryptographischen Absicherung der Kommunikation und Ablage überall erfolgt, wo es notwendig ist, um die Grundsätze der sicheren Softwarearchitektur zu unterstützen. Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere notwendig, wenn Daten mit hohem Schutzbedarf über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden. Um sicherzustellen, dass keine veralteten und als unsicher bekannten kryptographischen Lösungen verwendet werden, soll der Auftragnehmer die zulässigen kryptographischen Algorithmen mit ENERVIE abstimmen. Die zulässigen kryptographischen Lösungen richten sich nach BSI TR-02102 und sind auch gegen rechtliche Rahmenbedingungen zu prüfen.

7 Zutritts-, Zugangs- und Zugriffsrechte

Berechtigungen für den Zutritt zu Gebäuden oder Räumlichkeiten, den Zugang und/oder Zugriff auf Informationswerte oder Informationssysteme der ENERVIE werden nach Beantragung und Notwendigkeit gewährt und begrenzt. Die Einrichtung von zuvor genannten Berechtigungen erfolgt durch die ENERVIE und wird personalisiert vergeben. Jeder, der im Namen des Auftragnehmers agiert, der entfernten oder lokalen Zugriff auf Informationswerte der ENERVIE haben muss, muss Informationen (Vorname, Nachname, Mailadresse) zu seiner Identität bereitstellen. Der Auftragnehmer stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt. Jeder Mitarbeiter des Auftragnehmers muss sich mit seiner personalisierten Benutzerkennung anmelden. ENERVIE weist den Auftragnehmer darauf hin, dass Zutritt, Zugang und Zugriff protokolliert werden. Eine Weitergabe von personalisierten Benutzerkennungen und Kennwörtern ist untersagt. Die Verwendung der vergebenen Berechtigungen ist nur im Sinne und zum Zweck der Auftragserfüllung statthaft jegliche private Nutzung ist untersagt.

8 Netzwerksicherheit

Netzwerksegmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen müssen durch Sicherheitsmechanismen ausreichend voneinander getrennt werden. Netzwerkperimeter müssen einen Firewallschutz haben. Firewallregeln müssen einen dokumentierten Freigabeprozess durchlaufen. Authentisierungsmerkmale (Passwörter, PINs) dürfen nur verschlüsselt über das Netzwerk übermittelt werden. Aus dem Internet erreichbare administrative Zugänge für den technischen Zugriff müssen abgeschaltet oder durch eine 2-Faktor-Authentisierung angemessen abgesichert werden. Wenn drahtlose Netzwerke benutzt werden, müssen sie kryptographisch abgesichert sein. Es muss sichergestellt werden, dass die Systeme sich nicht mit unautorisierten Access-Points verbinden können bzw. dass keine unautorisierten Verbindungen aufgebaut und/oder zugelassen werden. Die Anbindung von Client-PCs eines Auftragnehmers oder seiner Subunternehmen in das Netzwerk der ENERVIE muss über einen Fernzugriff für Externe erfolgen. An Standorten der ENERVIE ist Auftragnehmern ausschließlich die Verwendung des für Gäste bereitgestellten WLAN oder der Zugriff auf das interne Netzwerk mit Standard-Clients der ENERVIE gestattet.

9 Fernzugriff für Externe

Der Prozess und die Funktion von Fernzugänge für Auftragnehmern zum Netzwerk der ENERVIE werden nur durch die ENERVIE definiert und unter den folgenden Bedingungen gestattet. Der Auftragnehmer muss sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Verfügbarkeit und Integrität der Assets, Services und Informationswerten der ENERVIE gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen, von denen der Auftragnehmer während eines Fernzugriffes Kenntnis erlangt hat. Der Auftragnehmer ist für alle Aktionen der Benutzerkonten mit Fernzugangsfunktion auf Systemen der ENERVIE verantwortlich und dokumentiert nachvollziehbar Ort, Datum, Zeit, Mitarbeiter und die durchgeführten Tätigkeiten. Wenn zum ENERVIE Netzwerk Verbindungen hergestellt werden, muss der Auftragnehmer

sicherstellen, dass ihr eigenes Netzwerk keinen unkontrollierten Zugriff durch Dritte auf das Netzwerk der ENERVIE ermöglicht.

10 Anforderungen an Softwareentwicklungsprozesse

Die Softwareentwicklungsprozesse des Auftragnehmers müssen so ausgelegt sein, dass der Sicherheit der entwickelten Software angemessene Beachtung in allen wichtigen Entwicklungsphasen geschenkt wird und die Prozesse sich an den allgemein anerkannten Industriestandards orientieren. Insbesondere sollen folgende Punkte berücksichtigt werden

- Vorhandene Standards der sicheren Softwarearchitektur und Programmierung
- Dokumentation der eingesetzten und angewendeten Standards
- Secure-Code-Reviews als Teil der Qualitätssicherung und zur Verfügung Stellung der Ergebnisse
- Angemessene Konfiguration, Dokumentation und Wartung von Open Source Komponenten
- Für Systeme, die aus nicht abgesicherten Netzen erreichbar sind, ist ein unabhängiger Sicherheitsnachweis zu erbringen

In Fällen, in denen der Auftragnehmer nur Anwendungen und/ oder andere Funktionalitäten liefert und ENERVIE für das Management auf den darunterliegenden Schichten verantwortlich ist, muss der Auftragnehmer eine kontinuierliche Funktionsfähigkeit seiner gelieferten Leistung auch bei Patches der darunterliegenden Schichten gewährleisten.

11 Anforderungen an Systeme

Der Auftragnehmer verpflichtet sich, die von ihm gelieferten Systeme zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren. Dies muss vor einer Systemabnahme durch den Auftraggeber geschehen sein.

Es wird von dem Auftragnehmer erwartet, folgende Komponenten des Betriebssystems oder anderer Software zu installieren:

- Software die für die Anwendung oder nach der Logik des Dienstes benötigt wird
- Software oder andere Anwendungen die aus der Integration mit anderen Services resultieren
- Software die aus Betriebs- und Wartungsanforderungen resultiert
- Jede andere Software darf nicht installiert werden

Die Installation weiterer Software ist nicht zulässig und nicht benötigte Netzwerkzugänge müssen deaktiviert sein. Die Nutzung jedes Zugangs muss in der Dokumentation des Auftragnehmers erläutert werden. Der Auftragnehmer stellt sicher, dass allgemeine Konfigurationsstandards (Best Practices) und Sicherheitsvorschriften eingehalten werden. Standardpasswörter in den von ihm installierten Systemen müssen geändert werden und im Rahmen seiner Möglichkeiten muss der Auftragnehmer sicherstellen, dass die von ihm gelieferten Systeme frei von „Backdoors" sind, die die verwendeten Sicherheitsmechanismen umgehen können.

12 Übertragung von Informationswerten

Werden zur Erfüllung des Auftrags Informationen auf Systeme des Auftragnehmers oder seiner Subunternehmer übertragen und/oder werden Informationen der ENERVIE auf Systemen des Auftragnehmers verarbeitet, hat der Auftragnehmer für Schutzmaßnahmen nach Stand der Technik zu sorgen. Der Auftragnehmer muss sicherstellen, dass auf der von ihm oder seiner Subunternehmen verwendeten und bereitgestellten Hardware die aktuellste Version eines Virenschutzsystems mit einer aktuellen Virensignatur-Datenbank installiert ist, die Schutz gegen Angriffe durch Schadsoftware via E-Mail, Web, mobile Datenträger oder anderen Medien bietet, indem sie den Dateizugriff kontrolliert. Im Weiteren müssen Systeme des Auftragnehmers einem Patch- und Vulnerability-Management unterliegen und über ein aktuelles und geeignetes Betriebssystem verfügen. Der Auftragnehmer muss sicherstellen, dass Informationen der ENERVIE auf dem Transportweg gegen Verlust, Veränderung und/oder Kenntnisnahme durch Unberechtigte nach Stand der Technik geschützt sind. Für den Austausch streng vertraulicher Informationen ist neben der Verschlüsselung auf dem Transportweg eine Inhaltsverschlüsselung Pflicht. Der Auftragnehmer muss angemessene Vorkehrungen zur physischen Sicherheit und zum Zutrittsschutz zu seinen Bereichen mit Informationswerten oder Systemen der ENERVIE treffen. Der Auftragnehmer muss Datensicherungs- und Wiederherstellungsprozesse etablieren und Datenwiederherstellungstests sind regelmäßig durchzuführen. Werden IT-Systeme oder Komponenten des Auftragnehmers, auf denen Daten der ENERVIE gespeichert sind, zur Reparatur gegeben oder einer Entsorgung zugeführt, muss gewährleistet sein, dass diese Daten nicht für Unberechtigte, auch nicht unter Verwendung von Daten-Wiederherstellungstechnologien, lesbar oder anderweitig auswertbar sind. Der Stand der Technik zur sicheren Vernichtung von Informationen ist nachweislich anzuwenden.

13 Audit

Der Auftragnehmer stimmt zu, dass ENERVIE oder ein durch ENERVIE beauftragter Dritter den Auftragnehmer in Bezug auf Informationssicherheit auditieren darf. Die Prüfungen werden auf der Grundlage der von dem Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden jeweils einvernehmlich vereinbart. Wird der Auftragnehmer aufgefordert eine Selbstauskunft zur Informationssicherheit zu liefern, ist hierfür die Dokumentenvorlage (IS Fragenkatalog.xlsx) der ENERVIE zu nutzen und binnen 10 Werktagen zu liefern. Abweichungen von den vereinbarten Sicherheitsanforderungen sind der ENERVIE unverzüglich zu melden.

14 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Vereinbarung nicht zutreffend sein, bleibt davon die Wirksamkeit der Vereinbarung im Übrigen unberührt. An die Stelle der nicht zutreffenden Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.